



Manual do usuário

Amazon Detective



Amazon Detective: Manual do usuário

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não são propriedade da Amazon pertencem aos respectivos proprietários, os quais podem ou não ser afiliados, estar conectados ou ser patrocinados pela Amazon.

Table of Contents

O que é o Detective?	1
Características do Amazon Detective	1
Acessando o Amazon Detective	3
Preços do Amazon Detective	5
Como o Detective funciona?	5
Quem usa o Detective?	6
Serviços relacionados	7
Conceitos básicos	9
Antes de começar	9
Inscreva-se para um Conta da AWS	9
Criar um usuário com acesso administrativo	10
Pré-requisitos	11
Conceder as permissões necessárias do Detective	11
O volume de dados da conta deve estar dentro da cota do Detective	12
AWS Command Line Interface Versão suportada	12
Recomendações	12
Alinhamento recomendado com e GuardDuty AWS Security Hub	12
Atualização recomendada da frequência GuardDuty CloudWatch de notificação	13
Habilitar o Detective	13
Habilitar o Detective (Console)	14
Habilitando o Detective (Detective API,) AWS CLI	15
Habilitando o Detective em todas as regiões (script Python ativado) GitHub	15
Verificar se os dados estão sendo extraídos	15
Conceitos e terminologia	17
Dados em um gráfico de comportamento	22
Como o Amazon Detective usa dados de origem para preencher um gráfico de comportamento	22
Como o Detective processa os dados de origem	23
Extração do Detective	23
Análise do Detective	23
Período de treinamento para novos gráficos de comportamento	24
Visão geral da estrutura de dados do gráfico de comportamento	25
Tipos de elementos na estrutura de dados do gráfico de comportamento	25
Tipos de entidades na estrutura de dados do gráfico de comportamento	26

Dados de origem usados em um gráfico de comportamento	31
Tipos de fontes de dados principais no Detective	32
Tipos de fontes de dados principais no Detective	33
Logs de auditoria do Amazon EKS para o Detective	34
AWS descobertas de segurança	35
Como o Detective faz a ingestão e armazena os dados de origem	36
Como o Detective aplica a cota de volume de dados aos gráficos de comportamento	37
Como o Detective é usado para investigações	39
Investigações de Detectives	39
Executando uma investigação de Detective	39
Analisar os relatórios de investigações	42
Compreendendo um relatório de Investigações de Detetives	43
Resumo do relatório de investigação	45
Baixar um relatório de investigação	45
Arquivar um relatório de investigação	46
Fases de investigação e pontos de partida	46
Fases da investigação	47
Pontos de partida para uma investigação de Detective	48
Fluxo de investigação de detetives	49
Analizando descobertas	51
Visão geral da descoberta	51
Escopo de tempo usado na visão geral de uma descoberta	51
Detalhes da descoberta	52
Entidades relacionadas	52
Solução de problemas de “Página não encontrada”	52
Encontrando grupos	53
Entender a página de grupos de descobertas	54
Descobertas informativas em grupos de descobertas	56
Perfis de grupos de descobertas	57
Visualização do grupo de descobertas	58
Resumo de grupo de descobertas	60
Analisar o resumo de grupos de descobertas	61
Desabilitar o resumo de grupo de descobertas	62
Habilitar o resumo de grupo de descobertas	63
Regiões compatíveis	63
Analizando entidades	64

Usar a página Resumo	64
Investigações	65
Geolocalizações recém-observadas	66
Grupos de descobertas ativos nos últimos 7 dias	66
Funções e usuários com o maior volume de chamadas de API	67
Instâncias do EC2 com o maior volume de tráfego	67
Clusters de contêiner com o maior número de pods do Kubernetes	68
Notificação de valor aproximado	68
Usando perfis de entidade	68
Escopo de tempo de um perfil de entidade	69
Identificador e tipo de entidade	69
Descobertas envolvidas	69
Grupos de descobertas envolvendo essa entidade	70
Painéis de perfil contendo detalhes da entidade e resultados de análises	70
Visualizar e interagir com painéis de perfil	70
Conteúdo do painel de perfil	71
Preferências de painéis de perfil	80
Mudar para outro console	81
Mudar para outro perfil de entidade	82
Explorar detalhes da atividade	82
Navegar diretamente até o perfil de uma entidade ou até a visão geral de uma descoberta	103
Ir a partir de outro console	103
Navegar usando um URL	106
Adicionar URLs do Detective para descobertas ao Splunk	109
Navegar por um perfil	110
Gerenciar o escopo de tempo	110
Definir datas e horários de início e de término específicos	111
Editar a duração do escopo de tempo	112
Definir o escopo de tempo para a janela de tempo de uma descoberta	112
Definir o escopo de tempo na página Resumo	113
Visualizar descobertas de uma entidade	113
Entidades de alto volume	114
O que é uma entidade de alto volume?	114
Visualizar a notificação de entidade de alto volume em um perfil	115
Visualizar a lista de entidades de alto volume para o escopo de tempo atual	115
Gerenciando descobertas e entidades	117

Procurar por uma descoberta ou entidade	117
Concluir a pesquisa	117
Usar os resultados da pesquisa	119
Solucionar problemas da pesquisa	120
Exportar dados do Detective	120
Arquivando uma descoberta GuardDuty	121
Gerenciar contas	122
Restrições e recomendações	123
Número máximo de contas-membro	123
Contas e regiões	123
Alinhamento das contas de administrador com o Security Hub e GuardDuty	123
Conceder as permissões necessárias para contas de administrador	124
Refletir as atualizações da organização no Detective	124
Transição para o Organizations	124
Designar a conta de administrador do Detective para a organização	125
Habilitar contas da organização como contas-membro	125
Designar a conta de administrador do Detective	126
Como a conta de administrador do Detective é gerenciada	126
Permissões necessárias para configurar a conta de administrador do Detective	128
Designar uma conta de administrador do Detective (console)	128
Designar uma conta de administrador do Detective (API do Detective, AWS CLI)	131
Remover uma conta de administrador do Detective (console)	131
Removendo a conta de administrador do Detective (Detective API,) AWS CLI	132
Removendo a conta de administrador delegado (Organizations API, AWS CLI)	133
Ações disponíveis para contas	133
Visualizar a lista de contas	135
Listar contas (Console)	137
Listando suas contas de membros (Detective API,) AWS CLI	138
Gerenciar contas-membro da organização	139
Habilitar novas contas da organização automaticamente	139
Habilitar contas da organização como contas-membro	141
Desassociar contas da organização	143
Gerenciar contas convidadas	145
Convidar contas-membro para um gráfico de comportamento	145
Habilitar uma conta-membro com status Não habilitado	150
Remover contas-membro convidadas de um gráfico de comportamento	152

Para contas-membro: gerenciar convites e associações	154
Política do IAM para uma conta-membro	154
Visualizar convites para gráficos de comportamento	155
Responder a um convite para um gráfico de comportamento	157
Remover sua conta de um gráfico de comportamento	159
Efeito das ações da conta	160
Detective desabilitado	160
Conta-membro removida do gráfico de comportamento	160
A conta-membro sai da organização	160
AWS conta suspensa	161
AWS conta fechada	161
Scripts em Python do Amazon Detective	162
Visão geral do script <code>enableDetective.py</code>	162
Visão geral do script <code>disableDetective.py</code>	163
Permissões necessárias para os scripts	163
Configurar o ambiente de execução dos scripts do Python	164
Criar uma lista em <code>.csv</code> de contas-membro a adicionar ou remover	167
Executar o <code>enableDetective.py</code>	167
Executar o <code>disableDetective.py</code>	168
Integração com o Amazon Security Lake	171
Antes de começar	173
Etapa 1: criar um assinante do Security Lake	173
Etapa 2: adicionar as permissões necessárias do IAM à sua conta	174
Etapa 3: aceitar o convite do ARN do compartilhamento de recursos e habilitar a integração ...	177
Criar uma pilha usando o modelo do AWS CloudFormation	177
Excluindo uma pilha CloudFormation	184
Alterar a configuração da integração	185
Desabilitar a integração	186
AWS Regiões suportadas	186
Consultar logs brutos no Detective	187
Consulte registros brutos para uma AWS função	191
Consulte registros brutos para um cluster Amazon EKS	191
Consultar logs brutos de uma instância do Amazon EC2	192
Segurança	193
Proteção de dados	194
Gerenciamento de chaves	195

Gerenciamento de identidade e acesso	195
Público	196
Autenticação com identidades	196
Gerenciamento do acesso usando políticas	199
Como o Amazon Detective funciona com o IAM	202
Exemplos de políticas baseadas em identidade	209
AWS políticas gerenciadas	215
Usar funções vinculadas a serviços	226
Solução de problemas de identidade e acesso	228
Registrar em log e monitoramento	230
Validação de conformidade	230
Resiliência	231
Segurança da infraestrutura	231
Melhores práticas de segurança	232
Melhores práticas para contas de administradores	232
Práticas recomendadas para contas-membro	232
Custos de previsão e monitoramento	233
Sobre a avaliação gratuita de gráficos de comportamento	233
Avaliação gratuita para fontes de dados opcionais	234
Uso e custo de uma conta de administrador	235
Volume de dados ingeridos para cada conta	235
Custos projetados para o gráfico de comportamento	236
Custo projetado para o gráfico de comportamento	236
Volume de dados ingeridos pelos pacotes de origem	236
Rastreamento do uso da conta-membro	237
Volume ingerido para cada gráfico de comportamento	237
Custo projetado em todos os gráficos de comportamento	238
Como o Detective calcula o custo projetado	238
Registrando chamadas da API Detective com CloudTrail	239
Informações de Detective em CloudTrail	240
Noções básicas sobre entradas de arquivos de log do Detective	241
Regiões e cotas	243
Regiões e endpoints do Detective	243
Cotas do Detective	243
Internet Explorer 11 não compatível	244
Como gerenciar tags	245

Visualizar as tags de um gráfico de comportamento (console)	245
Listar as tags de um gráfico de comportamento (API do Detective, AWS CLI)	245
Adicionar tags a um gráfico de comportamento (console)	246
Adicionar tags a um gráfico de comportamento (Detective API,) AWS CLI	246
Remover tags de um gráfico de comportamento (console)	247
Remover tags de um gráfico de comportamento (API do Detective, AWS CLI)	247
Desabilitar o Amazon Detective	248
Desabilitar o Detective (Console)	248
Desativando o Detective (Detective API,) AWS CLI	248
Desativando o Detective em todas as regiões (script Python ativado) GitHub	249
Histórico do documento	250
.....	cclxxvii

O que é o Amazon Detective?

O Amazon Detective ajuda a analisar, investigar e identificar rapidamente a causa raiz de descobertas de segurança ou atividades suspeitas. O Detective coleta automaticamente dados de log dos seus recursos da AWS. Em seguida, ele usa machine learning, análises estatísticas e a teoria de grafos para gerar visualizações que ajudam a realizar investigações de segurança eficazes com maior rapidez. O Detective faz a pré-construção de agregações de dados, resumos e contexto predefinidos que podem ajudar você a analisar e determinar a natureza e a extensão de possíveis problemas de segurança.

Com o Detective, você pode acessar até um ano de dados do histórico de eventos. Esses dados estão disponíveis por meio de um conjunto de visualizações que mostram mudanças no tipo e volume de atividade em uma janela de tempo selecionada. Detective vincula essas mudanças às GuardDuty descobertas. Para obter mais informações sobre os dados de origem no Detective, consulte [the section called “Dados de origem usados em um gráfico de comportamento”](#).

Ao agregar dados automaticamente e fornecer ferramentas visuais, o Amazon Detective permite que você conduza investigações de segurança mais rápidas e eficientes. Você pode analisar rapidamente possíveis problemas e determinar o escopo das ameaças à segurança.

Tópicos

- [Características do Amazon Detective](#)
- [Acessando o Amazon Detective](#)
- [Preços do Amazon Detective](#)
- [Como o Detective funciona?](#)
- [Quem usa o Detective?](#)
- [Serviços relacionados](#)

Características do Amazon Detective

Aqui estão algumas das principais maneiras pelas quais o Amazon Detective é útil para investigar atividades suspeitas em seu AWS ambiente e analisar recursos para identificar a causa raiz dos problemas de segurança.

Detective procurando grupos

[Detectives que buscam grupos](#) permitem que você examine várias atividades relacionadas a um possível evento de segurança. Você pode analisar a causa raiz das GuardDuty descobertas de alta severidade usando grupos de localização. Se um agente de ameaças está tentando comprometer seu AWS ambiente, ele normalmente executa uma sequência de ações que geram várias descobertas de segurança e comportamentos incomuns.

A página de busca de grupos no Detective exibe todos os grupos de descoberta relacionados extraídos do seu gráfico de comportamento na página de busca de grupos. Você pode observar [evidências](#) de diferentes tipos principais (como usuário do IAM ou função do IAM). Para alguns tipos de evidência, você pode observar evidências para todas as contas.

Detective fornece uma visualização interativa de cada grupo de descoberta para ajudá-lo a investigar problemas de segurança com mais rapidez e profundidade. A visualização foi projetada para exibir entidades e descobertas envolvidas em um incidente de segurança, facilitando a compreensão das conexões e das causas-raiz. Ajuda você a investigar problemas de forma mais rápida e completa com menos esforço. O painel de [Visualização](#) do grupo de descobertas exibe as descobertas e entidades envolvidas em um grupo de descobertas.

Detective Investigation para fazer a triagem dos resultados

Com o Detective Investigation, você pode investigar usuários e funções do IAM usando indicadores de comprometimento, que podem ajudá-lo a determinar se um recurso está envolvido em um incidente de segurança. Um indicador de comprometimento (IOC) é um artefato observado de ou em uma rede, um sistema ou um ambiente que pode (com alto nível de confiança) identificar atividades mal-intencionadas ou incidentes de segurança. Com as investigações de Detective, você pode maximizar a eficiência, focar nas ameaças à segurança e fortalecer as capacidades de resposta a incidentes.

O Detective Investigation usa modelos de aprendizado de máquina e inteligência de tópicos para identificar apenas os problemas mais críticos e suspeitos, permitindo que você se concentre em investigações de alto nível. Ele analisa automaticamente os recursos em seu AWS ambiente para identificar possíveis indicadores de comprometimento ou atividade suspeita. Isso permite identificar padrões e compreender quais recursos são afetados por eventos de segurança, oferecendo uma abordagem proativa para identificação e mitigação de ameaças.

Você pode iniciar uma investigação de detetive no console de detetives executando [uma](#) investigação de detetive. Para executar uma investigação programaticamente, use a

[StartInvestigation](#) operação da Detective API. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o comando [start-investigation](#).

Detective a integração com o Amazon Security Lake

O [Detective se integra ao Amazon Security Lake](#), o que significa que você pode consultar e recuperar os dados de log brutos armazenados pelo Security Lake. Com essa integração, você pode coletar registros e eventos das seguintes fontes, às quais o Security Lake oferece suporte nativo.

- AWS CloudTrail eventos de gerenciamento
- Logs de fluxo do Amazon Virtual Private Cloud (Amazon VPC)

Depois de integrar o Detective ao Security Lake, o Detective começa a extrair registros brutos do Security Lake relacionados a eventos de gerenciamento AWS CloudTrail e aos registros de fluxo do Amazon VPC. Você pode [consultar registros brutos](#) para ver os registros e eventos no Detective.

Investigue o volume de fluxo da VPC

Com o Detective, você pode examinar interativamente os [detalhes da atividade dos fluxos de rede da nuvem privada virtual \(VPC\) de suas instâncias do](#) Amazon Elastic Compute Cloud (Amazon EC2) e pods do Kubernetes. Detective coleta automaticamente os registros de fluxo de VPC de suas contas monitoradas, os agrega por instância do EC2 e apresenta resumos visuais e análises sobre esses fluxos de rede.

Para uma instância do EC2, os detalhes da atividade em Volume geral de fluxo do VPC mostram as interações entre a instância do EC2 e os endereços IP durante um intervalo de tempo selecionado.

Para um pod do Kubernetes, Volume geral de fluxo do VPC exibe o volume geral de bytes que entram e saem do endereço IP atribuído ao pod do Kubernetes para todos os endereços IP de destino.

Acessando o Amazon Detective

O Amazon Detective está disponível na maioria. Regiões da AWS Para obter uma lista das regiões em que o Detective está disponível atualmente, consulte os [endpoints e cotas do Amazon Detective](#) no. Referência geral da AWS Para obter informações sobre como gerenciar Regiões da AWS seu

Conta da AWS, consulte [Especificação de qual Regiões da AWS conta pode ser usada](#) no Guia de AWS Account Management referência.

Em cada região, você pode trabalhar com o Detective de qualquer uma das seguintes formas.

AWS Management Console

AWS Management Console É uma interface baseada em navegador que você pode usar para criar e gerenciar AWS recursos. Como parte desse console, o console do Amazon Detective fornece acesso à sua conta, dados e recursos de Detective. Você pode realizar qualquer tarefa de Detective usando o console do Detective — analise possíveis ameaças à segurança e analise, investigue e identifique a causa raiz das descobertas de segurança.

AWS ferramentas de linha de comando

Com as ferramentas de linha de AWS comando, você pode emitir comandos na linha de comando do seu sistema para realizar tarefas e AWS tarefas de Detective. Usar a linha de comando pode ser mais rápido e mais conveniente do que usar o console. As ferramentas da linha de comando também são úteis se você quiser criar scripts que realizem tarefas.

AWS fornece dois conjuntos de ferramentas de linha de comando: o AWS Command Line Interface (AWS CLI) e AWS Tools for PowerShell o. Para obter informações sobre como instalar e usar o AWS CLI, consulte o [Guia AWS Command Line Interface do usuário](#). Para obter informações sobre como instalar e usar as Ferramentas para PowerShell, consulte o [Guia AWS Tools for PowerShell do usuário](#).

AWS SDKs

AWS fornece SDKs que consistem em bibliotecas e exemplos de código para várias linguagens e plataformas de programação, por exemplo, Java, Go, Python, C++ e .NET. Os SDKs fornecem acesso conveniente e programático ao Detective e outros. Serviços da AWS Eles também incluem tarefas como assinatura criptográfica de solicitações, gerenciamento de erros e novas tentativas automáticas de solicitações. Para obter informações sobre como instalar e usar os AWS SDKs, consulte [Ferramentas para criar](#). AWS

API REST do Amazon Detective

A API REST do Amazon Detective oferece acesso abrangente e programático à sua conta, dados e recursos de Detective. Com essa API, você pode enviar solicitações HTTPS diretamente para o Detective. No entanto, diferentemente das ferramentas de linha de AWS comando e dos SDKs, o uso dessa API exige que seu aplicativo gerencie detalhes de baixo nível, como gerar um hash

para assinar uma solicitação. Para obter informações sobre essa API, consulte a Referência da [API Detective](#).

Preços do Amazon Detective

Assim como em outros AWS produtos, não há contratos ou compromissos mínimos para usar o Amazon Detective.

O preço do Detective é baseado em várias dimensões — e cobra uma taxa fixa escalonada por GB para todos os dados, independentemente da fonte. Para obter mais informações, consulte os preços [do Amazon Detective](#).

Para ajudar você a entender e prever o custo do uso do Detective, o Detective fornece uma estimativa dos custos de uso da sua conta. Você pode [revisar essas estimativas](#) no console do Amazon Detective e acessá-las com a API Amazon Detective. Dependendo de como você usa o serviço, você pode incorrer em custos adicionais pelo uso de outros Serviços da AWS em combinação com determinados recursos do Detective, como a integração com o Security Lake e o Detective Investigations.

Quando você ativa o Detective pela primeira vez, você Conta da AWS é automaticamente inscrito no teste gratuito de 30 dias do Detective. Isso inclui contas individuais habilitadas como parte de uma organização no AWS Organizations. Durante o teste gratuito, não há cobrança pelo uso do Detective na versão aplicável. Região da AWS

Para ajudá-lo a entender e prever o custo do uso do Detective após o término do teste gratuito, o Detective fornece custos de uso estimados com base no uso do Detective durante o teste. Seus dados de uso também indicam o tempo que resta até o término do teste gratuito. Você pode [analisar esses dados](#) no console do Amazon Detective e acessá-los com a API Amazon Detective.

Como o Detective funciona?

Detective extrai automaticamente eventos baseados em tempo, como tentativas de login, chamadas de API e tráfego de rede dos registros de fluxo da AWS CloudTrail Amazon VPC. Ele também ingere descobertas detectadas por GuardDuty.

A partir desses eventos, o Detective usa machine learning e visualizações para criar uma visão unificada e interativa dos comportamentos dos recursos e das interações entre eles ao longo do tempo. É possível explorar esse gráfico de comportamento para examinar ações díspares, como tentativas malsucedidas de login ou chamadas de API suspeitas. Você também pode ver como essas

ações afetam recursos como AWS contas e instâncias do Amazon EC2. Você pode ajustar o escopo e o cronograma do gráfico de comportamento para várias tarefas:

- Investigar rapidamente qualquer atividade fora do normal.
- Identificar padrões que possam indicar um problema de segurança.
- Entender todos os recursos afetados por uma descoberta.

As visualizações personalizadas do Detective fornecem uma linha de base e resumem as informações da conta. Essas descobertas podem ajudar a responder perguntas como “Essa é uma chamada de API incomum para essa função?” Ou “Esse aumento no tráfego dessa instância é esperado?”

Com o Detective, você não tem que organizar nenhum dado ou desenvolver, configurar ou ajustar suas próprias consultas e algoritmos. Não há nenhum custo inicial e você paga apenas pelos eventos analisados, sem nenhum software adicional para implantar ou outros feeds para assinar.

Quem usa o Detective?

Quando uma conta habilita o Detective, ela se torna a conta de administrador de um gráfico de comportamento. Um gráfico de comportamento é um conjunto vinculado de dados extraídos e analisados de uma ou mais AWS contas. Uma conta de administrador convida contas-membro para contribuir com seus dados no gráfico de comportamento da conta de administrador.

Detective também está integrado com AWS Organizations. A conta de gerenciamento da organização designa uma conta de administrador do Detective para a organização. A conta de administrador do Detective habilita as contas da organização como contas-membro no gráfico de comportamento da organização.

Para obter informações sobre como o Detective usa os dados de origem das contas em um gráfico de comportamento, consulte [the section called “Dados de origem usados em um gráfico de comportamento”](#).

Para obter informações sobre como as contas de administrador gerenciam gráficos de comportamento, consulte [Gerenciar contas](#). Para obter informações sobre como as contas-membro gerenciam seus convites e associações a gráficos de comportamento, consulte [the section called “Para contas-membro: gerenciar convites e associações”](#).

A conta do administrador usa as análises e visualizações geradas a partir do gráfico de comportamento para investigar AWS recursos e GuardDuty descobertas. Usando as integrações do

Detective com GuardDuty e AWS Security Hub, você pode passar de uma GuardDuty descoberta nesses serviços diretamente para o console do Detective.

Uma investigação do Detective se concentra na atividade conectada aos recursos da AWS envolvidos. Para obter uma visão geral do processo de investigação no Detective, consulte [Como o Amazon Detective é usado para investigações](#) no Guia do usuário do Detective.

Serviços relacionados

Para proteger ainda mais seus dados, cargas de trabalho e aplicativos AWS, considere usar o seguinte Serviços da AWS em combinação com o Amazon Detective.

AWS Security Hub

AWS Security Hub oferece uma visão abrangente do estado de segurança de seus AWS recursos e ajuda a verificar seu AWS ambiente em relação aos padrões e às melhores práticas de segurança do setor. Ele faz isso em parte consumindo, agregando, organizando e priorizando suas descobertas de segurança de vários produtos (Serviços da AWS incluindo Detective) e compatíveis da AWS Partner Network (APN). O Security Hub ajuda você a analisar suas tendências de segurança e identificar os problemas de segurança de maior prioridade em seu AWS ambiente.

Para saber mais sobre o Security Hub, consulte o [Guia do usuário da AWS Security Hub](#).

Amazon GuardDuty

GuardDuty A Amazon é um serviço de monitoramento de segurança que analisa e processa certos tipos de AWS registros, como registros de eventos de AWS CloudTrail dados para o Amazon S3 CloudTrail e registros de eventos de gerenciamento. Ele usa feeds de inteligência de ameaças, como listas de endereços IP e domínios maliciosos, e aprendizado de máquina para identificar atividades inesperadas, potencialmente não autorizadas e maliciosas em seu ambiente. AWS

Para saber mais sobre isso GuardDuty, consulte o [Guia GuardDuty do usuário da Amazon](#).

Amazon Security Lake

O Amazon Security Lake é um serviço de data lake de segurança totalmente gerenciado. Você pode usar o Security Lake para centralizar automaticamente os dados de segurança de AWS ambientes, provedores de SaaS, fontes locais, fontes de nuvem e fontes de terceiros em um data

lake específico que é armazenado em sua conta. AWS O Security Lake ajuda você a analisar dados de segurança, para que você tenha uma compreensão mais integral das posturas de segurança de toda a organização. Com o Security Lake, você também pode melhorar a proteção das suas workloads, aplicativos e dados.

Para saber mais sobre o Security Lake, consulte o [Guia do usuário do Amazon Security Lake](#). Para saber mais sobre como usar Detective e Security Lake juntos, consulte [Integração com o Amazon Security Lake](#)

Para saber mais sobre serviços AWS de segurança adicionais, consulte [Segurança, identidade e conformidade em AWS](#).

Introdução ao Amazon Detective

Este tutorial fornece uma introdução ao Amazon Detective. Você aprenderá como ativar o Detective em sua AWS conta. Você também aprenderá a verificar se o Detective começou a ingerir e extrair dados de sua AWS conta em seu gráfico de comportamento.

Quando você habilita o Amazon Detective, ele cria um gráfico de comportamento específico da região onde sua conta é a conta de administrador. Inicialmente, essa é a única conta no gráfico de comportamento. A conta do administrador pode então convidar outras AWS contas para contribuir com seus dados para o gráfico de comportamento. Consulte [Gerenciar contas](#).

Habilitar o Detective em uma região pela primeira vez também inicia uma avaliação gratuita de 30 dias do gráfico de comportamento. Se a conta desabilitar o Detective e o habilitar novamente, nenhuma avaliação gratuita estará disponível. Consulte [the section called “Sobre a avaliação gratuita de gráficos de comportamento”](#).

Após a avaliação gratuita, cada conta no gráfico de comportamento é cobrada pelos dados com os quais contribuiu. A conta de administrador pode rastrear o uso e ver o custo total projetado para um período típico de 30 dias em todo o gráfico de comportamento. Para ter mais informações, consulte [the section called “Uso e custo de uma conta de administrador”](#). As contas-membro podem rastrear o uso e o custo projetado dos gráficos de comportamento aos quais pertencem. Para ter mais informações, consulte [the section called “Rastreamento do uso da conta-membro”](#).

Tópicos

- [Antes de começar](#)
- [Pré-requisitos](#)
- [Recomendações](#)
- [Habilitar o Amazon Detective](#)
- [Verificar se os dados estão sendo extraídos](#)

Antes de começar

Antes de habilitar o Amazon Detective, é necessário ter uma Conta da AWS.

Inscreva-se para um Conta da AWS

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

Para se inscrever em um Conta da AWS

1. Abra <https://portal.aws.amazon.com/billing/signup>.
2. Siga as instruções on-line.

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

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

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando <https://aws.amazon.com/> e selecionando Minha conta.

Criar um usuário com acesso administrativo

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

Proteja seu Usuário raiz da conta da AWS

1. Faça login [AWS Management Console](#) como proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.

Para obter ajuda ao fazer login usando o usuário-raiz, consulte [Signing in as the root user](#) (Fazer login como usuário-raiz) no Guia do usuário do Início de Sessão da AWS .

2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

Para obter instruções, consulte [Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz \(console\) no Guia](#) do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

Para obter instruções, consulte [Habilitar AWS IAM Identity Center](#) no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

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

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

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

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

Para obter instruções, consulte [Create a permission set](#) no Guia do usuário do AWS IAM Identity Center .

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

Para obter instruções, consulte [Add groups](#) no Guia do usuário do AWS IAM Identity Center .

Pré-requisitos

Certifique-se de que os seguintes requisitos sejam atendidos.

Conceder as permissões necessárias do Detective

Antes de habilitar o Detective, você deve se certificar de que sua entidade principal do IAM tenha as permissões necessárias do Detective. A entidade principal pode ser um usuário ou uma função que você já esteja usando, ou você pode criar um novo usuário ou função para usar no Detective.

Quando você se cadastra na Amazon Web Services (AWS), sua conta é automaticamente cadastrada em todos os Serviços da AWS, inclusive no Amazon Detective. No entanto, para habilitar e usar o Detective, é necessário configurar permissões que permitam o acesso às operações da API e ao console do Amazon Detective. Você ou seu administrador podem fazer isso usando AWS Identity and Access Management (IAM) para anexar a [política AmazonDetectiveFullAccess gerenciada](#) ao seu diretor do IAM, que concede acesso a todas as ações do Detective.

O volume de dados da conta deve estar dentro da cota do Detective

O volume de dados que flui para um gráfico de comportamento deve ser menor que o máximo permitido pelo Detective.

Ao tentar habilitar o Detective, se o volume de dados da sua conta for muito grande, você não poderá habilitar o Detective. O console do Detective exibe uma notificação para indicar que o volume de dados é muito grande.

AWS Command Line Interface Versão suportada

Para usar o AWS CLI para realizar tarefas de Detective, a versão mínima exigida é 1.16.303.

Recomendações

Alinhamento recomendado com o GuardDuty AWS Security Hub

Se você estiver inscrito em GuardDuty e AWS Security Hub, recomendamos que sua conta seja uma conta de administrador para esses serviços. Se as contas de administrador forem as mesmas para os três serviços, os seguintes pontos de integração funcionarão perfeitamente.

- No Security Hub GuardDuty ou no Security Hub, ao visualizar os detalhes de uma GuardDuty descoberta, você pode passar dos detalhes da descoberta para o perfil de descoberta do Detective.
- Em Detective, ao investigar uma GuardDuty descoberta, você pode escolher a opção de arquivar essa descoberta.

Se você tiver contas de administrador diferentes no Security Hub GuardDuty e no Security Hub, recomendamos que você alinhe as contas de administrador com base no serviço que você usa com mais frequência.

- Se você usa com GuardDuty mais frequência, habilite Detective usando a conta de GuardDuty administrador.

Se você usa AWS Organizations para gerenciar contas, designe a conta do GuardDuty administrador como a conta do administrador Detective da organização.

- Se você usa o Security Hub com mais frequência, habilite o Detective usando a conta de administrador do Security Hub.

Se você usa o Organizations para gerenciar as contas, designe a conta de administrador do Security Hub como a conta de administrador do Detective para a organização.

Se não puder usar as mesmas contas de administrador em todos os serviços, depois de habilitar o Detective, você poderá optar por criar uma função entre contas. Essa função concede a uma conta de administrador acesso a outras contas.

Para obter informações sobre como o IAM oferece suporte a esse tipo de função, consulte [Fornecer acesso a um usuário do IAM em outra AWS conta que você possui](#) no Guia do usuário do IAM.

Atualização recomendada da frequência GuardDuty CloudWatch de notificação

Em GuardDuty, os detectores são configurados com uma frequência de CloudWatch notificação da Amazon para relatar ocorrências subsequentes de uma descoberta. Isso inclui o envio de notificações ao Detective.

Por padrão, a frequência é de seis horas. Isso significa que, mesmo que uma descoberta se repita muitas vezes, as novas ocorrências não são refletidas no Detective até seis horas depois.

Para reduzir o tempo necessário para o Detective receber essas atualizações, recomendamos que a conta do GuardDuty administrador altere a configuração de seus detectores para 15 minutos. Observe que alterar a configuração não afeta o custo de uso GuardDuty.

Para obter informações sobre como definir a frequência de notificação, consulte [Monitoring GuardDuty Findings with Amazon CloudWatch Events](#) no Guia GuardDuty do usuário da Amazon.

Habilitar o Amazon Detective

Você pode habilitar o Detective a partir do console do Detective, da API do Detective ou do AWS Command Line Interface.

Você só pode habilitar o Detective uma vez em cada região. Se você já for a conta de administrador de um gráfico de comportamento na região, não poderá habilitar o Detective novamente nessa região.

Habilitar o Detective (Console)

Você pode habilitar o Amazon Detective no AWS Management Console.

Para habilitar o Detective (console)

1. Faça login no AWS Management Console. Em seguida, abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. Escolha Comece a usar.
3. Na página Habilitar Amazon Detective, Align admin accounts (recomendado) explica a recomendação de alinhar as contas de administrador entre Detective e Amazon e. GuardDuty AWS Security Hub Consulte [the section called “Alinhamento recomendado com e GuardDuty AWS Security Hub”](#).
4. O botão Anexar política do IAM leva você diretamente ao console do IAM e abre a política recomendada. Você tem a opção de anexar a política recomendada ao principal usado como Detective. Se você não tem permissões para operar no console do IAM, vá em Permissões recomendadas, copie o nome do recurso da Amazon (ARN) da política e forneça-o ao administrador do IAM. A política poderá ser anexada em seu nome.

Confirme se a política do IAM necessária está em vigor.

5. A seção Adicionar tags permite que você adicione tags ao gráfico de comportamento.

Para adicionar uma tag, faça o seguinte:

- a. Selecione Adicionar nova tag.
- b. Em Chave, insira o nome da tag.
- c. Em Valor, insira o valor da tag.

Para remover uma tag, clique na opção Remover da tag.

6. Escolha Habilitar o Amazon Detective.
7. Depois de habilitar o Detective, você pode convidar contas-membro para o gráfico de comportamento.

Para navegar até a página Gerenciamento de contas, escolha Adicionar membros agora. Para obter informações sobre como convidar contas-membro, consulte [the section called “Convidar contas-membro para um gráfico de comportamento”](#).

Habilitando o Detective (Detective API,) AWS CLI

Você pode habilitar o Amazon Detective na API do Detective ou no AWS Command Line Interface.

Para ativar o Detective (Detective API,) AWS CLI

- API do Detective: use a operação [CreateGraph](#).
- AWS CLI: na linha de comando, execute o comando [create-graph](#).

```
aws detective create-graph --tags '{"tagName": "tagValue"}
```

O comando a seguir habilita o Detective e define o valor da tag Department como Security.

```
aws detective create-graph --tags '{"Department": "Security"}
```

Habilitando o Detective em todas as regiões (script Python ativado) GitHub

Detective fornece um script de código aberto GitHub que faz o seguinte:

- Habilita o Detective para uma conta de administrador em uma lista especificada de regiões
- Adiciona uma lista de contas-membro a cada um dos gráficos de comportamento resultantes
- Envia e-mails de convite para as contas-membro
- Aceita automaticamente os convites para as contas-membro

Para obter informações sobre como configurar e usar os GitHub scripts, consulte [the section called “Scripts em Python do Amazon Detective”](#).

Verificar se os dados estão sendo extraídos

Depois de ativar o Detective, ele começa a ingerir e extrair dados da sua AWS conta em seu gráfico de comportamento.

Para a extração inicial, os dados geralmente ficam disponíveis no gráfico de comportamento em 24 horas.

Uma forma de verificar se o Detective está extraindo dados é procurar exemplos de valores na página Pesquisar do Detective.

Para verificar exemplos de valores na página Pesquisar

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, selecione Pesquisar.
3. No menu Selecionar tipo, escolha um tipo de item.

A opção Exemplos de seus dados contém um conjunto de amostras de identificadores do tipo selecionado que estão nos dados do gráfico de comportamento.

Se você conseguir ver exemplos de valores, saberá que está ocorrendo a ingestão e extração dos dados em seu gráfico de comportamento.

Conceitos e terminologia do Amazon Detective

Os seguintes termos e conceitos são importantes para entender como o Amazon Detective funciona.

Conta de administrador

O Conta da AWS que possui um gráfico de comportamento e que usa o gráfico de comportamento para investigação.

Uma conta de administrador convida contas-membro para contribuírem com seus dados no gráfico de comportamento. Para ter mais informações, consulte [the section called “Convidar contas-membro para um gráfico de comportamento”](#).

Para o gráfico de comportamento da organização, a conta de administrador é a conta de administrador do Detective designada pela conta de gerenciamento da organização. Para ter mais informações, consulte [the section called “Designar a conta de administrador do Detective”](#). A conta de administrador do Detective pode habilitar qualquer conta da organização como uma conta-membro no gráfico de comportamento. Para ter mais informações, consulte [the section called “Gerenciar contas-membro da organização”](#).

As contas de administrador também podem visualizar o uso de dados do gráfico de comportamento e remover contas-membro desse gráfico.

Organização do Sistema Autônomo (ASO)

A organização intitulada à qual um sistema autônomo é atribuído. Esse sistema autônomo é uma rede heterogênea ou um conjunto de redes que usam lógica e políticas de roteamento semelhantes.

Gráfico de comportamento

Um conjunto de dados vinculado gerado a partir de dados de origem recebidos que é associado a uma ou mais Contas da AWS.

Cada gráfico de comportamento usa a mesma estrutura de descobertas, entidades e relacionamentos.

Conta de administrador delegada ()AWS Organizations

No Organizations, a conta de administrador delegado de um serviço consegue gerenciar o uso de um serviço para a organização.

No Detective, a conta de administrador do Detective também é a conta de administrador delegado, a menos que a conta de administrador do Detective seja a conta de gerenciamento da organização. A conta de gerenciamento da organização não pode ser uma conta de administrador delegado.

No Detective, a autodelegação é permitida. Uma conta de gerenciamento da organização pode delegar sua própria conta como o administrador delegado do Detective, mas isso seria registrado ou lembrado apenas no escopo do Detective, e não do Organizations.

Conta de administrador de Detective

A conta designada pela conta de gerenciamento da organização para ser a conta de administrador do gráfico de comportamento da organização em uma região. Para ter mais informações, consulte [the section called “Designar a conta de administrador do Detective”](#).

O Detective recomenda que a conta de gerenciamento da organização escolha uma conta diferente de sua própria conta.

Se a conta não for a conta de gerenciamento da organização, a conta de administrador do Detective também será a conta de administrador delegado para o Detective no Organizations.

Dados de origem do Detective

Versões processadas e estruturadas de informações dos seguintes tipos de feeds:

- Registros de AWS serviços, como AWS CloudTrail logs e Amazon VPC Flow Logs
- GuardDuty descobertas

O Detective usa os dados de origem do Detective para preencher o gráfico de comportamento. Também armazena cópias dos dados de origem do Detective para apoiar suas análises.

Entidade

Um item extraído dos dados ingeridos.

Cada entidade tem um tipo, que identifica o tipo de objeto que ela representa. Exemplos de tipos de entidades incluem endereços IP, instâncias do Amazon EC2 e AWS usuários.

As entidades podem ser AWS recursos que você gerencia ou endereços IP externos que interagiram com seus recursos.

Para cada entidade, os dados de origem também são usados para preencher as propriedades da entidade. Os valores das propriedades podem ser extraídos diretamente dos registros de origem ou agregados em vários registros.

Descoberta

Um problema de segurança detectado pela Amazon GuardDuty.

Grupo de descobertas

Uma coleção de descobertas, entidades e evidências relacionadas que podem se referir ao mesmo evento ou problema de segurança. O Detective gera grupos de descobertas com base em um modelo de machine learning integrado.

Evidência do Detective

O Detective identifica evidências adicionais relacionadas a um grupo de descobertas com base em dados em seu gráfico de comportamento coletados nos últimos 45 dias. Essa evidência é apresentada como uma descoberta com o valor de severidade Informativo. Uma evidência fornece informações de apoio que destacam uma atividade incomum ou um comportamento desconhecido que é potencialmente suspeito quando visto em um grupo de descobertas. Um exemplo disso podem ser geolocalizações recém-observadas ou chamadas de API observadas dentro do escopo de tempo de uma descoberta. No momento, essas descobertas só podem ser visualizadas no Detective e não são enviadas ao Security Hub.

Visão geral da descoberta

Uma única página que fornece um resumo das informações sobre uma descoberta.

A visão geral de uma descoberta contém uma lista de entidades envolvidas na descoberta. Na lista, você pode ir para o perfil de uma entidade.

A visão geral de uma descoberta também contém um painel de detalhes com os atributos da descoberta.

Entidade de alto volume

Uma entidade que tem conexões a ou de um grande número de outras entidades durante um intervalo de tempo. Por exemplo, uma instância do EC2 pode ter conexões a partir de milhões de endereços IP. O número de conexões excede o limite que o Detective pode acomodar.

Quando o escopo de tempo atual contém um intervalo de tempo de alto volume, o Detective notifica o usuário.

Para obter mais informações, consulte [Visualizar detalhes de entidades de alto volume](#) no Guia do usuário do Amazon Detective.

Investigação

O processo de triagem de atividades suspeitas ou interessantes, que determina seu escopo, chega à origem ou causa subjacente e, em seguida, determina como proceder.

Conta-membro

É uma Conta da AWS que uma conta de administrador convidou para contribuir com dados para um gráfico de comportamento. No gráfico de comportamento da organização, uma conta-membro pode ser uma conta da organização que a conta de administrador do Detective habilitou como conta-membro.

As contas-membro convidadas podem responder ao convite para o gráfico de comportamento e remover as próprias contas do gráfico de comportamento. Para ter mais informações, consulte [the section called “Para contas-membro: gerenciar convites e associações”](#).

As contas da organização não podem alterar sua associação ao gráfico de comportamento da organização.

Todas as contas-membro também podem visualizar as informações de uso de suas contas nos gráficos de comportamento para os quais contribuem com dados.

Elas não têm outro acesso ao gráfico de comportamento.

Gráfico de comportamento organizacional

O gráfico de comportamento que pertence à conta de administrador do Detective. A conta de gerenciamento da organização designa a conta de administrador do Detective. Para ter mais informações, consulte [the section called “Designar a conta de administrador do Detective”](#).

No gráfico de comportamento da organização, a conta de administrador do Detective controla se uma conta da organização é uma conta-membro. Uma conta da organização não pode se remover do gráfico de comportamento da organização.

A conta de administrador do Detective também pode convidar outras contas para o gráfico de comportamento da organização.

Perfil

Uma única página que fornece uma coleção de visualizações de dados relacionadas à atividade de uma entidade.

Para descobertas, os perfis ajudam os analistas a determinarem se a descoberta é uma preocupação genuína ou um falso positivo.

Os perfis fornecem informações para apoiar uma investigação sobre uma descoberta ou para uma busca geral por atividades suspeitas.

Painel de perfil

Uma única visualização em um perfil. Cada painel de perfil tem como objetivo ajudar a responder uma pergunta ou perguntas específicas para auxiliar um analista em uma investigação.

Os painéis de perfil podem conter pares de valores-chave, tabelas, cronogramas, gráficos de barras ou gráficos de geolocalização.

Relacionamento

Atividade que ocorre entre entidades individuais. Os relacionamentos também são extraídos dos dados de origem recebidos.

Semelhante a uma entidade, um relacionamento tem um tipo, que identifica os tipos de entidades envolvidas e a direção da conexão. Um exemplo de tipo de relacionamento é um endereço IP conectado a uma instância do Amazon EC2.

Escopo de tempo

A janela de tempo usada para definir o escopo dos dados exibidos nos perfis.

O escopo de tempo padrão de uma descoberta reflete a primeira e a última vez em que a atividade suspeita foi observada.

O escopo de tempo padrão do perfil de uma entidade são as 24 horas anteriores.

Dados em um gráfico de comportamento

No Amazon Detective, você conduz investigações usando dados de um gráfico de comportamento do Detective.

Um gráfico de comportamento é um conjunto vinculado de dados gerados a partir dos dados de origem do Detective que são ingeridos de uma ou mais contas da Amazon Web Services (AWS).

O gráfico de comportamento usa os dados de origem para fazer o seguinte:

- Gerar um panorama de seus sistemas, usuários e das interações entre eles ao longo do tempo
- Realizar uma análise mais detalhada de atividades específicas para ajudar você a responder às perguntas que surgirem durante a condução de investigações
- Correlacionar coleções de descobertas, entidades e evidências que podem se referir ao mesmo evento ou problema de segurança.

Observe que toda extração, modelagem e análise de dados do gráfico de comportamento ocorre dentro do contexto de cada gráfico de comportamento individual.

Para obter informações sobre como uma conta de administrador gerencia as contas dos membros em um gráfico de comportamento, consulte [Gerenciamento de contas](#).

Conteúdo

- [Como o Amazon Detective usa dados de origem para preencher um gráfico de comportamento](#)
- [Período de treinamento para novos gráficos de comportamento](#)
- [Visão geral da estrutura de dados do gráfico de comportamento](#)
- [Dados de origem usados em um gráfico de comportamento](#)

Como o Amazon Detective usa dados de origem para preencher um gráfico de comportamento

Para fornecer os dados brutos para investigações, o Detective reúne dados de todo o seu ambiente da AWS e de outros lugares, inclusive o seguinte:

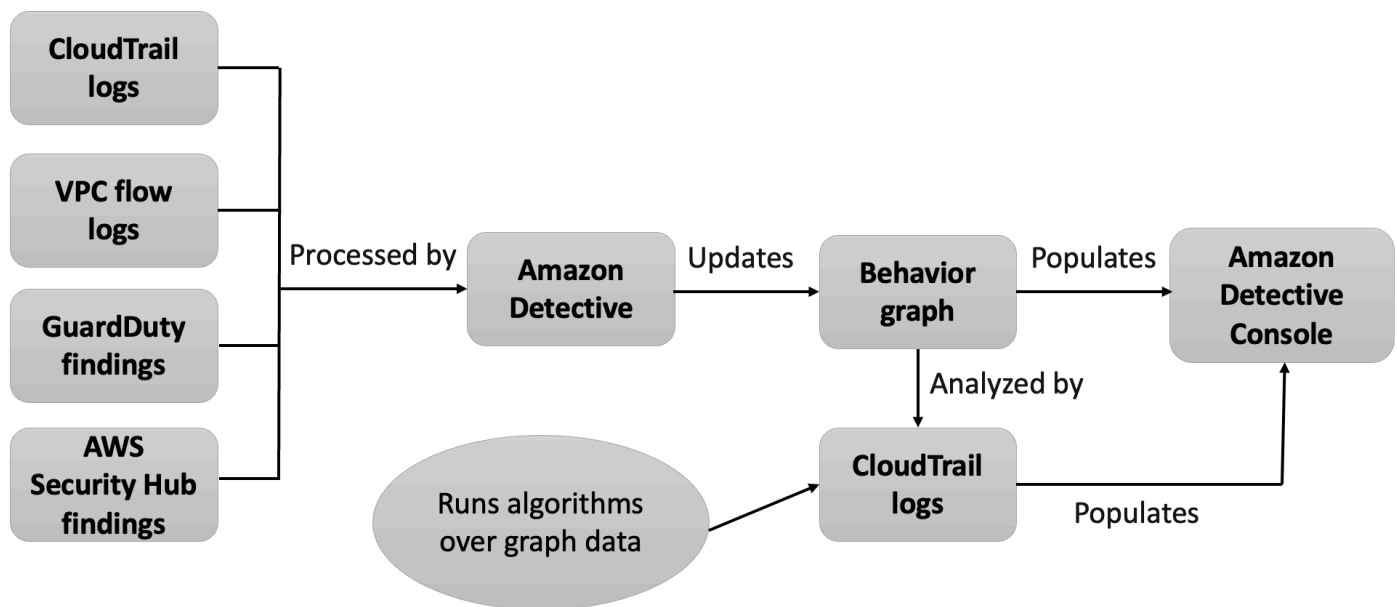
- Dados de log, incluindo Amazon Virtual Private Cloud (Amazon VPC) e AWS CloudTrail
- Descobertas da Amazon GuardDuty

- Descobertas de AWS Security Hub

Para saber mais sobre os dados de origem usados em um gráfico de comportamento, consulte [Dados de origem usados em um gráfico de comportamento](#).

Como o Detective processa os dados de origem

À medida que novos dados chegam, o Detective usa uma combinação de extração e análise para preencher o gráfico de comportamento.



Extração do Detective

A extração é baseada em regras de mapeamento configuradas. Uma regra de mapeamento basicamente diz: “Sempre que você ver esse dado, use-o dessa forma específica para atualizar os dados do gráfico de comportamento”.

Por exemplo, um registro de dados de origem do Detective recebido pode incluir um endereço IP. Se isso acontecer, o Detective usa as informações desse registro para criar uma nova entidade de endereço IP ou atualizar uma entidade de endereço IP existente.

Análise do Detective

As análises são algoritmos mais complexos que analisam os dados para fornecer informações sobre as atividades associadas às entidades.

Por exemplo, um tipo de análise do Detective analisa a frequência com que a atividade ocorre por meio da execução de algoritmos. Para entidades que fazem chamadas de API, o algoritmo procura chamadas de API que a entidade normalmente não usa. O algoritmo também busca um grande aumento no número de chamadas de API.

Os insights analíticos apoiam as investigações ao fornecerem respostas às principais perguntas dos analistas e são frequentemente usados para preencher painéis de perfil de descobertas e entidades.

Período de treinamento para novos gráficos de comportamento

Uma via de investigação de uma descoberta é comparar a atividade durante o escopo de tempo da descoberta com a atividade que ocorreu antes da descoberta ser detectada. Atividades que não foram vistas antes podem ser mais propensas a serem suspeitas.

Alguns painéis de perfil do Amazon Detective destacam atividades que não foram observadas durante o período anterior à descoberta. Vários painéis de perfil também exibem um valor de linha de base para mostrar a atividade média durante os 45 dias anteriores ao escopo de tempo. O tempo do escopo é o resumo da atividade de uma entidade ao longo do tempo.

À medida que mais dados são extraídos para o gráfico de comportamento, o Detective desenvolve uma imagem mais precisa de qual atividade é normal em sua organização e qual atividade é incomum.

No entanto, para criar essa imagem, o Detective precisa acessar pelo menos duas semanas de dados. A maturidade da análise do Detective também aumenta com o número de contas no gráfico de comportamento.

As primeiras duas semanas após a habilitação do Detective são consideradas um período de treinamento. Durante esse período, painéis de perfil que comparam a atividade do escopo de tempo com a atividade anterior exibem uma mensagem de que o Detective está em um período de treinamento.

Durante o período de teste, o Detective recomenda que você adicione o máximo possível de contas de membros ao gráfico de comportamento. Isso fornece ao Detective um conjunto maior de dados, o que permite gerar uma imagem mais precisa da atividade normal de sua organização.

Visão geral da estrutura de dados do gráfico de comportamento

A estrutura de dados do gráfico de comportamento define a estrutura dos dados extraídos e analisados. Também define como os dados de origem são mapeados para o gráfico de comportamento.

Tipos de elementos na estrutura de dados do gráfico de comportamento

A estrutura de dados do gráfico de comportamento tem os seguintes elementos de informação.

Entidade

Uma entidade representa um item extraído dos dados de origem do Detective.

Cada entidade tem um tipo, que identifica o tipo de objeto que ela representa. Exemplos de tipos de entidades incluem endereços IP, instâncias do Amazon EC2 e AWS usuários.

Para cada entidade, os dados de origem também são usados para preencher as propriedades da entidade. Os valores das propriedades podem ser extraídos diretamente dos registros de origem ou agregados em vários registros.

Algumas propriedades consistem em um único valor escalar ou agregado. Por exemplo, para uma instância do EC2, o Detective rastreia o tipo de instância e o número total de bytes processados.

As propriedades das séries temporais rastreiam a atividade ao longo do tempo. Por exemplo, para uma instância do EC2, o Detective rastreia ao longo do tempo as portas exclusivas que foram usadas.

Relacionamentos

Um relacionamento representa a atividade que ocorre entre entidades individuais. Os relacionamentos também são extraídos dos dados de origem do Detective.

Semelhante a uma entidade, um relacionamento tem um tipo, que identifica os tipos de entidades envolvidas e a direção da conexão. Um exemplo de tipo de relacionamento é um endereço IP conectado a instâncias do EC2.

Para cada relacionamento individual, como um endereço IP específico conectado a uma instância específica, o Detective rastreia as ocorrências ao longo do tempo.

Tipos de entidades na estrutura de dados do gráfico de comportamento

A estrutura de dados do gráfico de comportamento consiste em tipos de entidade e relacionamento que fazem o seguinte:

- Rastreiam os servidores, endereços IP e agentes de usuário que estão sendo usados
- Acompanhe os AWS usuários, funções e contas que estão sendo usados
- Rastreiam as conexões de rede e as autorizações que ocorrem no ambiente da AWS

A estrutura de dados do gráfico de comportamento contém os seguintes tipos de entidade.

AWS conta

AWS contas que estão presentes nos dados de origem do Detective.

Para cada conta, o Detective responde a várias perguntas:

- Quais chamadas de API a conta usou?
- Quais agentes de usuário a conta usou?
- Quais organizações do sistema autônomo (ASOs) a conta usou?
- Em quais localizações geográficas a conta está ativa?

AWS papel

AWS funções que estão presentes nos dados de origem do Detective.

Para cada função, o Detective responde a várias perguntas:

- Quais chamadas de API a função usou?
- Quais agentes de usuário a função usou?
- Quais ASOs a função usou?
- Em quais localizações geográficas a função está ativa?
- Quais recursos assumiram essa função?
- Quais funções essa função assumiu?
- Quais sessões de função envolveram essa função?

AWS usuário

AWS usuários que estão presentes nos dados de origem do Detective.

Para cada usuário, o Detective responde a várias perguntas:

- Quais chamadas de API o usuário usou?
- Quais agentes de usuário o usuário usou?
- Em quais localizações geográficas o usuário está ativo?
- Quais funções esse usuário assumiu?
- Quais sessões de função envolveram esse usuário?

Usuário federado

Instâncias de um usuário federado. Os exemplos de usuários federados incluem o seguinte:

- Uma identidade que faz login usando Security Assertion Markup Language (SAML)
- Uma identidade que faz login usando a federação de identidades da web

Para cada usuário federado, o Detective responde a várias perguntas:

- Com qual provedor de identidade o usuário federado se autenticou?
- Qual foi o público do usuário federado? O público identifica o aplicativo que solicitou o token de identidade da web do usuário federado.
- Em quais localizações geográficas o usuário federado está ativo?
- Quais agentes de usuário o usuário federado usou?
- Quais ASOs o usuário federado usou?
- Quais funções esse usuário federado assumiu?
- Quais sessões de função envolveram esse usuário federado?

EC2 instance (Instância do EC2)

Instâncias do EC2 presentes nos dados de origem do Detective.

Para instâncias do EC2, o Detective responde a várias perguntas:

- Quais endereços IP se comunicaram com a instância?
- Quais portas foram usadas para se comunicar com a instância?
- Qual volume de dados foi enviado de e para a instância?
- Qual VPC contém a instância?
- Quais chamadas de API a instância do EC2 usou?
- Quais agentes de usuário a instância do EC2 usou?

- Quais ASOs a instância do EC2 usou?
- Em quais localizações geográficas a instância do EC2 está ativa?
- Quais funções a instância do EC2 assumiu?

Sessão de função

Instâncias de um recurso que está assumindo uma função. Cada sessão de função é identificada pelo identificador da função e pelo nome da sessão.

Para cada função, o Detective responde a várias perguntas:

- Quais recursos estavam envolvidos nessa sessão de função? Em outras palavras, qual função foi assumida e qual recurso assumiu a função?

Observe que, para funções assumidas entre contas, o Detective não consegue identificar o recurso que assumiu a função.

- Quais chamadas de API a sessão de função usou?
- Quais agentes de usuário a sessão de função usou?
- Quais ASOs a sessão de função usou?
- Em quais localizações geográficas a sessão de função está ativa?
- Qual usuário ou função iniciou essa sessão de função?
- Quais sessões de função iniciaram a partir dessa sessão de função?

Descoberta

Descobertas descobertas pela Amazon GuardDuty que são inseridas nos dados de origem do Detective.

Para cada descoberta, o Detective rastreia o tipo de descoberta, a origem e a janela de tempo da atividade da descoberta.

Também armazena informações específicas da descoberta, como funções ou endereços IP envolvidos na atividade detectada.

Endereço IP

Endereços IP presentes nos dados de origem do Detective.

Para cada endereço IP, o Detective responde a várias perguntas:

- Quais chamadas de API o endereço usou?
- Quais portas o endereço usou?
- Quais usuários e agentes de usuário usaram o endereço IP?
- Em quais localizações geográficas o endereço IP está ativo?
- A quais instâncias do EC2 esse endereço IP foi atribuído e com as quais se comunicou?

Bucket do S3

Buckets do S3 que estão nos dados de origem do Detective.

Para cada bucket do S3, o Detective responde a várias perguntas:

- Quais entidades principais interagiram com o bucket do S3?
- Quais chamadas de API foram feitas para o bucket do S3?
- De quais localizações geográficas as entidades principais fizeram chamadas de API para o bucket do S3?
- Quais agentes de usuário foram usados para interagir com o bucket do S3?
- Quais ASOs foram usados para interagir com o bucket do S3?

Você pode excluir um bucket do S3 e, em seguida, criar um novo bucket com o mesmo nome. Como o Detective usa o nome do bucket do S3 para identificá-lo, ele os trata como uma única entidade do bucket do S3. No perfil da entidade, o Horário de criação é o primeiro horário de criação. O Horário de exclusão é o horário de exclusão mais recente.

Para visualizar todos os eventos de criação e exclusão, defina o escopo de tempo para começar com o horário de criação e terminar com o horário de exclusão. No painel de perfil Volume geral de chamadas de API, exiba os detalhes da atividade para o escopo de tempo. Filtre os métodos da API para mostrarem os métodos Create e Delete. Consulte [the section called “Volume geral de chamadas de API”](#).

Agente de usuário

Agentes de usuário presentes nos dados de origem do Detective.

Para cada agente de usuário, o Detective responde a perguntas como as seguintes:

- Quais chamadas de API o agente de usuário usou?
- Quais usuários e funções usaram o agente de usuário?
- Quais endereços IP usaram o e agente de usuário?

Cluster do EKS

Clusters do EKS presentes nos dados de origem do Detective.

Note

Para ver detalhes completos desse tipo de entidade, a fonte de dados opcional dos logs de auditoria do EKS deve estar habilitada. Para obter mais informações, consulte [Fontes de dados opcionais](#)

Para cada cluster do EKS, o Detective responde a perguntas como as seguintes:

- Quais chamadas de API do Kubernetes foram executadas nesse cluster?
- Quais usuários e contas de serviço (sujeitos) do Kubernetes estão ativos nesse cluster?
- Quais contêineres foram iniciados nesse cluster?
- Quais imagens são usadas para iniciar contêineres nesse cluster?

Pod do Kubernetes

Pods do Kubernetes presentes nos dados de origem do Detective.

Note

Para ver detalhes completos desse tipo de entidade, a fonte de dados opcional dos logs de auditoria do EKS deve estar habilitada. Para obter mais informações, consulte [Fontes de dados opcionais](#)

Para cada pod, o Detective responde a perguntas como as seguintes:

- Quais imagens de contêiner nesse pod são comuns em minhas contas?
- Qual atividade foi direcionada a esse pod?
- Quais contêineres funcionam nesse pod?
- Os registros dos contêineres nesse pod são comuns em minhas contas?
- Quais outros contêineres estão funcionando nos outros pods do workload?
- Há algum contêiner anômalo nesse pod que não esteja nos outros pods do workload?

Imagem de contêiner

Imagens de contêiner presentes nos dados de origem do Detective.

Note

Para ver detalhes completos desse tipo de entidade, a fonte de dados opcional dos logs de auditoria do EKS deve estar habilitada. Para obter mais informações, consulte [Fontes de dados opcionais](#)

Para cada imagem de contêiner, o Detective responde a perguntas como as seguintes:

- Quais outras imagens no meu ambiente compartilham o mesmo repositório ou registro com essa imagem?
- Quantas cópias dessa imagem estão sendo executadas no meu ambiente?

Sujeito do Kubernetes

Sujeitos do Kubernetes presentes nos dados de origem do Detective. Um sujeito do Kubernetes é um usuário ou conta de serviço.

Note

Para ver detalhes completos desse tipo de entidade, a fonte de dados opcional dos logs de auditoria do EKS deve estar habilitada. Para obter mais informações, consulte [Fontes de dados opcionais](#)

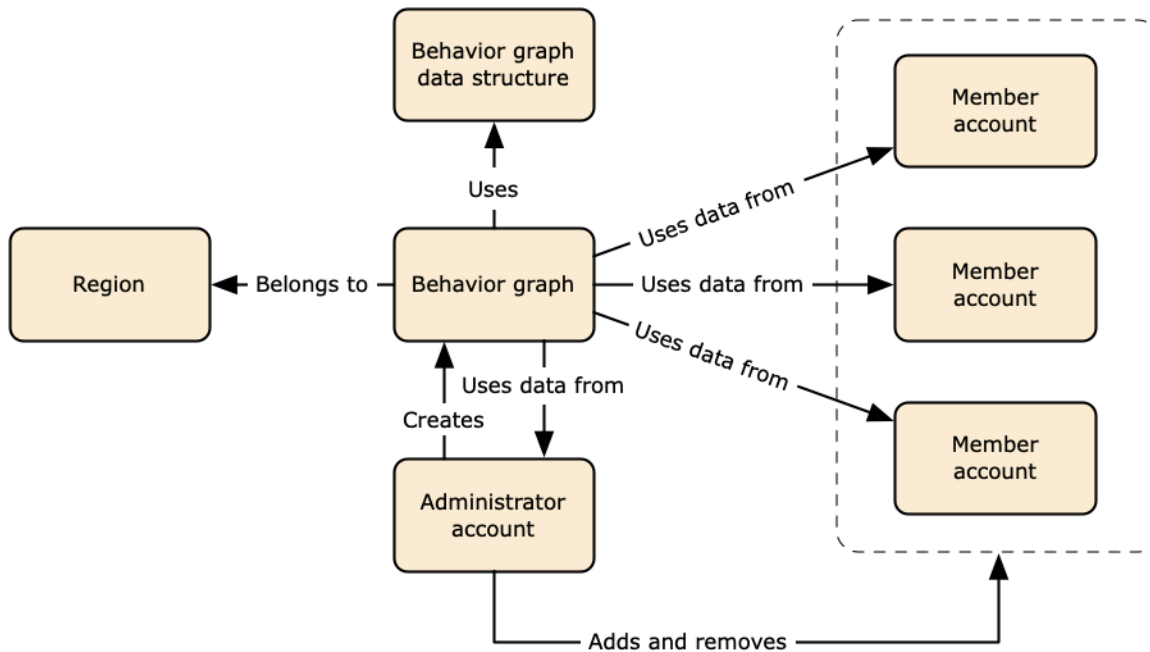
Para cada sujeito, o Detective responde a perguntas como as seguintes:

- Quais entidades principais do IAM foram autenticadas como esse sujeito?
- Quais descobertas estão associadas a esse sujeito?
- Quais endereços IP o sujeito está usando?

Dados de origem usados em um gráfico de comportamento

Para preencher um gráfico de comportamento, o Amazon Detective usa dados de origem da conta de administrador e das contas-membro do gráfico de comportamento.

Com o Detective, você pode acessar até um ano de dados do histórico de eventos. Esses dados estão disponíveis por meio de um conjunto de visualizações que mostram mudanças no tipo e volume de atividade em uma janela de tempo selecionada. Detective vincula essas mudanças às GuardDuty descobertas.



Para obter detalhes sobre a estrutura de dados do gráfico de comportamento, consulte [Visão geral da estrutura de dados do gráfico de comportamento](#) no Guia do usuário do Detective.

Tipos de fontes de dados principais no Detective

Detective ingere dados desses tipos de registros: AWS

- AWS CloudTrail troncos
- Logs de fluxo do Amazon Virtual Private Cloud (Amazon VPC)
 - Ingere registros IPv4 e IPv6, mas não registros MAC produzidos pelos Elastic Fabric Adapters.
 - Ingere registros de registro quando o valor do `log-status` campo está no OK estado. Para obter mais informações, consulte [Registros de log de fluxo](#) no Guia do usuário da Amazon VPC.
 - Ingere registros de fluxo produzidos por instâncias do Amazon Elastic Compute Cloud executadas somente nessas VPCs. Nenhum outro recurso, como gateways NAT, instâncias RDS ou clusters Fargate, é usado.
 - Ingere tráfego aceito e rejeitado.
- Para contas cadastradas GuardDuty, o Detective também GuardDuty ingere as descobertas.

Detective consome e registra eventos de fluxo de CloudTrail VPC usando fluxos independentes e duplicativos de registros de fluxo de VPC. CloudTrail Esses processos não afetam nem usam suas configurações de log de fluxo existentes CloudTrail e de VPC. Eles também não afetam o desempenho nem aumentam seus custos com esses serviços.

Tipos de fontes de dados principais no Detective

O Detective oferece pacotes de origem opcionais, além das três fontes de dados oferecidas no pacote principal do Detective (o pacote principal inclui registros AWS CloudTrail , registros de fluxo de VPC e descobertas). GuardDuty Um pacote de fonte de dados opcional pode ser iniciado ou interrompido para um gráfico de comportamento a qualquer momento.

O Detective oferece uma avaliação gratuita de 30 dias para todos os pacotes de origem principais e opcionais por região.

Note

O Detective retém todos os dados recebidos de cada pacote de fonte de dados por até 1 ano.

Atualmente, os seguintes pacotes de origem opcionais estão disponíveis:

- Logs de auditoria do EKS

Esse pacote de fonte de dados opcional permite que o Detective consuma informações detalhadas sobre clusters do EKS em seu ambiente e adicione esses dados ao seu gráfico de comportamento. Detective correlaciona as atividades do usuário com eventos de CloudTrail gerenciamento da AWS e atividades de rede com os registros de fluxo do Amazon VPC sem a necessidade de você habilitar ou armazenar esses registros manualmente. Para mais detalhes, consulte [Logs de auditoria do Amazon EKS para o Detective](#).

- AWS descobertas de segurança

Esse pacote de fonte de dados opcional permite que o Detective consuma dados do Security Hub e os adicione ao gráfico de comportamento. Para mais detalhes, consulte [AWS descobertas de segurança](#).

Iniciar ou interromper uma fonte de dados opcional:

1. Abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, em Configurações, selecione Geral.
3. Em Pacotes de origem opcionais, selecione Atualizar. Em seguida, selecione a fonte de dados que você deseja habilitar ou desmarque uma caixa para uma fonte de dados já habilitada e escolha Atualizar para alterar quais pacotes de fontes de dados estão habilitados.

Note

Se você parar e reiniciar uma fonte de dados opcional, verá uma lacuna nos dados exibidos em alguns perfis de entidade. Essa lacuna será anotada na tela do console e representará o período em que a fonte de dados foi interrompida. Quando uma fonte de dados é reiniciada, o Detective não faz a ingestão de dados retroativamente.

Logs de auditoria do Amazon EKS para o Detective

Logs de auditoria do Amazon EKS são um pacote de origem de dados opcional que pode ser adicionado ao seu gráfico de comportamento do Detective. Você pode visualizar os pacotes de origem opcionais disponíveis e seu status na sua conta na página Configurações no console ou por meio da API do Detective.

Uma avaliação gratuita de 30 dias é fornecida para essa fonte de dados. Para saber mais, consulte [Avaliação gratuita para fontes de dados opcionais](#).

A habilitação dos logs de auditoria do Amazon EKS permite que o Detective adicione informações detalhadas sobre recursos criados com o Amazon EKS ao seu gráfico de comportamento. Essa fonte de dados aprimora as informações fornecidas sobre os seguintes tipos de entidade: cluster do EKS, pod do Kubernetes, imagem do contêiner e sujeitos do Kubernetes.

Além disso, se você habilitou os registros de auditoria do EKS como fonte de dados na Amazon, GuardDuty poderá ver detalhes das descobertas do Kubernetes em GuardDuty. Para obter mais informações sobre como ativar essa fonte de dados, GuardDuty consulte Proteção do [Kubernetes na Amazon. GuardDuty](#)

Note

Essa fonte de dados é habilitada por padrão para novos gráficos de comportamento criados após 26 de julho de 2022. Para gráficos de comportamento criados antes de 26 de julho de 2022, ela deve ser habilitada manualmente.

Adicionar ou remover logs de auditoria do Amazon EKS como fonte de dados opcional:

1. Abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, em Configurações, selecione Geral.
3. Em Pacotes de origem, selecione Logs de auditoria do EKS para habilitar essa fonte de dados. Se já estiver habilitada, selecione-o novamente para parar a ingestão de logs de auditoria do EKS no gráfico de comportamento.

AWS descobertas de segurança

AWS as descobertas de segurança são um pacote de fonte de dados opcional que pode ser adicionado ao seu gráfico de comportamento de Detective.

Você pode visualizar os pacotes de origem opcionais disponíveis e seu status na sua conta na página Configurações no console ou por meio da API do Detective.

Uma avaliação gratuita de 30 dias é fornecida para essa fonte de dados. Para saber mais, consulte [Avaliação gratuita para fontes de dados opcionais](#).

Habilitar as descobertas de segurança da AWS permite que o Detective use as descobertas do Security Hub agregadas pelo Security Hub a partir de serviços upstream em um formato padrão de descobertas chamado AWS Security Format (ASFF), o que elimina a necessidade de esforços demorados de conversão de dados. Ele correlaciona as descobertas ingeridas nos produtos para priorizar as mais importantes.

Adicionar ou remover descobertas AWS de segurança como fonte de dados opcional:

Note

A fonte de dados de descobertas de AWS segurança é ativada por padrão para novos gráficos de comportamento criados após 16 de maio de 2023. Para gráficos de comportamento criados antes de 16 de maio de 2023, ela deve ser habilitada manualmente.

1. Abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, em Configurações, selecione Geral.
3. Em Pacotes de origem, selecione descobertas AWS de segurança para habilitar essa fonte de dados. Se já estiver habilitada, selecione-o novamente para interromper a ingestão das descobertas do AWS Security Finding Format (ASFF) em seu gráfico de comportamento.

Descobertas atualmente compatíveis

Detective ingere todas as descobertas do ASFF no Security Hub de serviços que são de propriedade da Amazon ou AWS

- Para ver a lista de integrações de serviços compatíveis, consulte Integrações de [serviços da AWS disponíveis](#) no Guia do AWS Security Hub usuário.
- Para ver a lista de recursos compatíveis, consulte [Recursos](#) no Guia do usuário do AWS Security Hub .
- AWS As descobertas de serviços com um status de conformidade não definido FAILED e as descobertas agregadas entre regiões não são ingeridas.

Como o Detective faz a ingestão e armazena os dados de origem

Quando o Detective está habilitado, ele começa a ingestão dos dados de origem da conta de administrador do gráfico de comportamento. À medida que as contas-membro são adicionadas ao gráfico de comportamento, o Detective também começa a usar os dados dessas contas-membro.

Os dados de origem do Detective consistem em versões estruturadas e processadas dos feeds originais. Para apoiar a análise do Detective, ele armazena cópias dos dados de origem do Detective.

O processo de ingestão do Detective alimenta os dados nos buckets do Amazon Simple Storage Service (Amazon S3) no armazenamento de dados de origem do Detective. À medida que novos dados de origem chegam, outros componentes do Detective coletam os dados e iniciam os processos de extração e análise. Para obter mais informações, consulte [Como o Detective usa os dados de origem para preencher um gráfico de comportamento](#) no Guia do usuário do Detective.

Como o Detective aplica a cota de volume de dados aos gráficos de comportamento

O Detective tem cotas rígidas no volume de dados que permite em cada gráfico de comportamento. O volume de dados é a quantidade de dados diária que flui para o gráfico de comportamento do Detective.

O Detective aplica essas cotas quando uma conta de administrador habilita o Detective e quando uma conta-membro aceita um convite para contribuir em um gráfico de comportamento.

- Se o volume de dados de uma conta de administrador exceder 10 TB por dia, a conta de administrador não poderá habilitar o Detective.
- Se o volume de dados adicionado de uma conta-membro fizer com que o gráfico de comportamento exceda 10 TB por dia, a conta-membro não poderá ser habilitada.

O volume de dados de um gráfico de comportamento também pode crescer naturalmente com o tempo. O Detective verifica diariamente o volume de dados do gráfico de comportamento para garantir que ele não exceda a cota.

Se o volume de dados do gráfico de comportamento estiver se aproximando da cota, o Detective exibirá uma mensagem de aviso no console. Para evitar exceder a cota, você pode remover contas-membro.

Se o volume de dados do gráfico de comportamento exceder 10 TB por dia, você não poderá adicionar novas contas-membro ao gráfico de comportamento.

Se o volume de dados do gráfico de comportamento exceder 15 TB por dia, o Detective interrompe a ingestão de dados no gráfico de comportamento. A cota diária de 15 TB reflete tanto o volume de dados normal quanto os picos no volume de dados. Quando essa cota é atingida, nenhum dado novo é inserido no gráfico de comportamento, mas os dados existentes não são removidos. Você ainda pode usar o histórico desses dados para investigação. O console exibe uma mensagem para indicar que a ingestão de dados está suspensa para o gráfico de comportamento.

Se a ingestão de dados for suspensa, você deverá trabalhar com ela AWS Support para reativá-la. Se possível, antes de entrar em contato AWS Support, tente remover as contas dos membros para que o volume de dados fique abaixo da cota. Isso facilita a reativação da ingestão de dados no gráfico de comportamento.

Como o Amazon Detective é usado para investigações

O Amazon Detective facilita a análise, investigação e identificação rápida da causa raiz de descobertas de segurança ou atividades suspeitas. Se você é iniciante no Detective, consulte [O que é o Amazon Detective?](#) e [conceitos e terminologia do Amazon Detective](#).

Tópicos

- [Investigações de Detectives](#)
- [Fases de investigação e pontos de partida](#)
- [Fluxo de investigação do Amazon Detective](#)

Investigações de Detectives

Você pode usar o recurso Amazon Detective Investigations para investigar usuários e funções do IAM usando indicadores de comprometimento, que podem ajudá-lo a determinar se um recurso está envolvido em um incidente de segurança. Um indicador de comprometimento (IOC) é um artefato observado de ou em uma rede, um sistema ou um ambiente que pode (com alto nível de confiança) identificar atividades mal-intencionadas ou incidentes de segurança. Com o Detective Investigations, você pode maximizar a eficiência, focar nas ameaças à segurança e fortalecer as capacidades de resposta a incidentes.

Detective Investigations usa modelos de aprendizado de máquina e inteligência de ameaças para analisar automaticamente os recursos em seu AWS ambiente e identificar possíveis incidentes de segurança. Elas permitem que você use de forma proativa, eficaz e eficiente a automação criada com base no gráfico comportamental do Detective para melhorar as operações de segurança. Usando o Detective Investigations, você pode investigar táticas de ataque, viagens impossíveis, endereços IP sinalizados e encontrar grupos. A investigação executa as etapas iniciais de investigação de segurança e gera um relatório que destaca os riscos identificados pelo Detective para ajudar você a entender os eventos de segurança e responder a possíveis incidentes.

Executando uma investigação de Detective

Use Executar investigação para analisar recursos, como usuários e perfis do IAM, e para gerar um relatório de investigação. O relatório gerado detalha o comportamento anômalo que indica um possível comprometimento.

Console

Siga estas etapas para executar uma investigação de detetive na página Investigações usando o console Amazon Detective.

1. Faça login no AWS Management Console. Em seguida, abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, selecione Investigações.
3. Na página Investigações, escolha Executar investigação no canto superior direito.
4. Na seção Selecionar recurso, você tem três maneiras de realizar uma investigação. Você pode optar por realizar a investigação de um recurso recomendado pelo Detective. Você pode executar a investigação de um recurso específico. Você também pode investigar um recurso na página Pesquisar do Detective.

1. Choose a recommended resource— Detective recomenda recursos com base em sua atividade em descobertas e grupos de localização. Para executar a investigação de um recurso recomendado pelo Detective, na tabela Recursos recomendados, selecione um recurso para investigar.

A tabela de Recursos recomendados fornece os seguintes detalhes:

- ARN do recurso — O nome do recurso da Amazon (ARN) do recurso. AWS
 - Motivo de investigação: exibe os principais motivos para investigar o recurso. Os motivos pelos quais o Detective recomenda investigar um recurso são os seguintes:
 - Se um recurso esteve envolvido em uma descoberta de alta gravidade nas últimas 24 horas.
 - Se um recurso esteve envolvido em um grupo de descobertas observado nos últimos sete dias. Os grupos de descobertas do Detective permitem que você examine várias atividades relacionadas a um possível evento de segurança. Para obter mais detalhes, consulte [the section called “Encontrando grupos”](#).
 - Se um recurso esteve envolvido em uma descoberta nos últimos sete dias.
 - Última descoberta: as descobertas mais recentes são priorizadas no topo da lista.
 - Tipo de recurso: identifica o tipo de recurso. Por exemplo, um AWS usuário ou uma AWS função.
2. Specify an AWS role or user with an ARN— Você pode selecionar uma AWS função ou AWS usuário e executar uma investigação para o recurso específico.

Siga estas etapas para investigar um tipo específico de recurso.

- a. Na lista suspensa Selecionar tipo de recurso, escolha AWS função ou AWS usuário.
 - b. Insira o ARN do recurso do IAM. Para obter mais detalhes sobre ARNs de recursos, consulte [Amazon Resource Names \(ARNs\)](#) no Guia do usuário do IAM.
3. Find a resource to investigate from the Search page— Você pode pesquisar todos os seus recursos do IAM na página Detective Search.

Siga estas etapas para investigar um recurso na página de pesquisa.

- a. No painel de navegação, selecione Pesquisar.
 - b. Na página de pesquisa, pesquise um recurso do IAM.
 - c. Navegue até a página de perfil do recurso e execute a investigação a partir daí.
5. Na seção Tempo do escopo da investigação, escolha o Tempo do escopo da investigação para avaliar a atividade do recurso selecionado. Você pode selecionar uma data de início e hora de início e uma data de término e hora de término no formato UTC. A janela do tempo de escopo vai de no mínimo de 3 horas e no máximo de 30 dias.
6. Selecione Executar investigação.

API

Para executar uma investigação programaticamente, use a [StartInvestigation](#) operação da Detective API. Se você estiver usando o AWS Command Line Interface (AWS CLI), execute o comando [start-investigation](#).

Em sua solicitação, use os seguintes parâmetros para executar uma investigação no Detective:

- `GraphArn`: especifica o nome do recurso da Amazon (ARN) do gráfico de comportamento.
- `EntityArn`: especifica o nome do recurso da Amazon (ARN) exclusivo do usuário do IAM e do perfil do IAM.
- `ScopeStartTime`: opcionalmente, especifique os dados e a hora em que a investigação deve começar. O valor é uma string formatada em UTC ISO8601. Por exemplo, `2021-08-18T16:35:56.284Z`.
- `ScopeEndTime`: opcionalmente, especifique os dados e a hora em que a investigação deve terminar. O valor é uma string formatada em UTC ISO8601. Por exemplo, `2021-08-18T16:35:56.284Z`.

Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

```
aws detective start-investigation \  
--graph-arn arn:aws:detective:us-  
east-1:123456789123:graph:fdac8011456e4e6182facb26dfceade0  
--entity-arn arn:aws:iam::123456789123:role/rolename --scope-start-  
time 2023-09-27T20:00:00.00Z  
--scope-end-time 2023-09-28T22:00:00.00Z
```

Você também pode realizar uma investigação nas seguintes páginas no Detective:

- Página de perfil de um usuário do IAM ou de um perfil do IAM no Detective.
- Painel de visualização gráfica de um grupo de descobertas.
- Coluna de ações de um recurso envolvido.
- Usuário do IAM ou perfil do IAM em uma página de descobertas.

Depois que o Detective executa a investigação de um recurso, um relatório de investigação é gerado. Para acessar o relatório, acesse Investigações no painel de navegação.

Analisar os relatórios de investigações

Os relatórios de investigações permitem que você analise os relatórios gerados de investigações realizadas anteriormente no Detective.

Como analisar os relatórios de investigações

1. Faça login no AWS Management Console. Em seguida, abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, selecione Investigações.

Anote atributos a seguir de um relatório de investigação.

- ID: o identificador gerado do relatório de investigações. Selecione esse ID para ler um resumo do relatório da investigação que contém os detalhes da investigação.
- Status: cada investigação é associada a um status com base no status de conclusão da investigação. Os valores de status podem ser Em andamento, Com êxito ou Com falha.

- **Gravidade:** cada investigação recebe um nível de gravidade. O Detective atribui automaticamente uma gravidade à descoberta.

Uma gravidade representa a disposição analisada pela investigação de um único recurso em um determinado tempo de escopo. A gravidade relatada por uma investigação não implica nem indica o caráter crítico ou a importância que um recurso afetado pode ter para sua organização.

Os valores de gravidade de descobertas da investigação podem ser Crítico, Alto, Médio, Baixo ou Informativo, do mais ao menos grave.

As investigações com valor de gravidade Crítico ou Alto devem ser priorizadas para inspeção posterior, já que elas têm mais chances de representar problemas de segurança de alto impacto identificados pelo Detective.

- **Entidade:** a coluna Entidade contém detalhes sobre as entidades específicas detectadas na investigação. Algumas entidades são AWS contas, como usuário e função.
- **Status:** a coluna de data de Criação contém detalhes sobre a data e a hora em que o relatório de investigação foi criado pela primeira vez.

Compreendendo um relatório de Investigações de Detetives

Um relatório da Detective Investigations lista um resumo do comportamento incomum ou da atividade maliciosa que indica comprometimento. Ele também lista as recomendações sugeridas pelo Detective para reduzir o risco de segurança.

Admin report summary Info High

We observed anomalous behavior for the role from [redacted] indicating potential compromise. The role invoked CloudTrail management actions mapped to Impact MITRE tactic(s). The role was also involved in Findings that map to the MITRE tactic(s) Discovery, as well as other tactic(s). The role was also involved in 10 findings, 1 finding group, 170 impossible travels, 3 new geolocations, and 5 new user agents.

<p>Scope time</p> <p>05/25/2023 13:00 UTC - 05/31/2023 19:00 UTC</p> <p>role</p> <p>[redacted]</p>	<p>Indicators of compromise</p> <p>5 Tactics</p> <p>0 Flagged IP</p> <p>170 Impossible travel</p> <p>1 Finding group</p>	<p>Recommendation</p> <p>Based on our investigation, we recommend you take action to mitigate what we've found on AWS role Admin. Please review Security Best Practices in IAM to secure your AWS resource.</p>
--	--	---

Como visualizar um relatório de investigação de um ID de investigação específico.

1. Faça login no AWS Management Console. Em seguida, abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, selecione Investigações.
3. Na tabela Relatórios, selecione um ID de investigação.

O Detective gera o relatório para o tempo de Escopo e o Usuário selecionados. O relatório contém uma seção de Indicadores de comprometimento que incluem detalhes sobre um ou mais dos indicadores de comprometimento listados abaixo. Ao analisar cada indicador de comprometimento, você pode selecionar um item para detalhar e revisar seus detalhes.

- **Táticas, técnicas e procedimentos:** identifica táticas, técnicas e procedimentos (TTPs) usados em um possível evento de segurança. A estrutura MITRE ATT&CK é usada para entender os TTPs. As táticas são baseadas na matriz [MITRE ATT&CK Matrix for Enterprise](#).
- **Endereços IP sinalizados pela Inteligência de ameaças:** endereços IP suspeitos são sinalizados e identificados como ameaças críticas ou graves com base na inteligência de ameaças do Detective.
- **Atividade humanamente impossível:** detecta e identifica atividades incomuns e impossíveis de serem realizadas pelo usuário em uma conta. Por exemplo, esse indicador lista uma mudança drástica entre a origem e a localização de destino de um usuário em um curto espaço de tempo.
- **Grupo de descobertas relacionado:** mostra diversas atividades relacionadas a um possível evento de segurança. O Detective usa técnicas de análise de gráficos que infere relacionamentos entre descobertas e entidades e os agrupa como um grupo de descobertas.
- **Descobertas relacionadas:** atividades relacionadas associadas a um possível evento de segurança. Lista todas as categorias distintas de evidências que estão conectadas ao recurso ou ao grupo de descobertas.
- **Novas geolocalizações:** identifica novas geolocalizações usadas no nível do recurso ou da conta. Por exemplo, esse indicador lista uma geolocalização observada que é uma localização pouco frequente ou não utilizada com base na atividade anterior do usuário.
- **Novos agentes de usuário:** identifica novos agentes de usuário usados no nível do recurso ou da conta.
- **Novas ASOs:** identifica novas Organizações de sistemas autônomos (ASOs) usadas no nível do recurso ou da conta. Por exemplo, esse indicador lista uma nova organização atribuída como uma ASO.

Resumo do relatório de investigação

O resumo de investigação destaca indicadores anômalos que exigem atenção, de acordo com o tempo de escopo selecionado. Com o resumo, você pode identificar mais rapidamente a causa raiz de possíveis problemas de segurança, identificar padrões e entender os recursos afetados pelos eventos de segurança.

No resumo detalhado do relatório de investigação, você pode visualizar os detalhes a seguir.

Visão geral das investigações

No painel Visão geral, você pode visualizar os IPs com atividade de alto nível de gravidade, o que pode fornecer mais contexto sobre caminho que um invasor seguiu.

O Detective destaca Atividade incomum na investigação, por exemplo, a impossibilidade de viagem de uma fonte para um destino distante pelo usuário do IAM.

O Detective mapeia as investigações de acordo com táticas, técnicas e procedimentos (TTPs) usados em um possível evento de segurança. A estrutura MITRE ATT&CK é usada para entender os TTPs. As táticas são baseadas na matriz [MITRE ATT&CK Matrix for Enterprise](#).

Indicadores de investigação

Você pode usar as informações no painel Indicadores para determinar se um recurso da AWS está envolvido em atividades incomuns que podem indicar comportamento mal-intencionado e seu impacto. Um indicador de comprometimento (IOC) é um artefato observado de ou em uma rede, um sistema ou um ambiente que pode (com alto nível de confiança) identificar atividades mal-intencionadas ou incidentes de segurança.

Baixar um relatório de investigação

Você pode baixar o relatório Detective Investigations no formato JSON para analisá-lo mais detalhadamente ou armazená-lo em sua solução de armazenamento preferida, como um bucket Amazon S3.

Como baixar um relatório de investigação da tabela Relatórios.

1. Faça login no AWS Management Console. Em seguida, abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, selecione Investigações.
3. Selecione uma investigação na tabela Relatórios e selecione Baixar.

Como baixar um relatório de investigação na página de resumo.

1. Faça login no AWS Management Console. Em seguida, abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, selecione Investigações.
3. Selecione uma investigação na tabela Relatórios.
4. Na página de resumo das investigações, selecione Baixar.

Arquivar um relatório de investigação

Ao concluir a investigação no Amazon Detective, você pode arquivar o relatório da investigação. Uma investigação arquivada indica que você concluiu a análise da investigação.

Apenas um Administrador do Detective pode arquivar ou desarquivar uma investigação. O Detective armazena as investigações arquivadas por 90 dias.

Como arquivar um relatório de investigação da tabela Relatórios.

1. Faça login no AWS Management Console. Em seguida, abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, selecione Investigações.
3. Selecione uma investigação na tabela Relatórios e selecione Arquivar.

Como arquivar um relatório de investigação na página de resumo.

1. Faça login no AWS Management Console. Em seguida, abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, selecione Investigações.
3. Selecione uma investigação na tabela Relatórios.
4. Na página de resumo das investigações, selecione Arquivar.

Fases de investigação e pontos de partida

O Amazon Detective fornece ferramentas para apoiar o processo geral de uma investigação. Uma investigação no Detective pode começar com uma descoberta, um grupo de descoberta ou uma entidade.

Fases da investigação

Qualquer processo de investigação envolve as seguintes fases:

Triagem

O processo de investigação começa quando você é notificado sobre uma instância suspeita de atividade maliciosa ou de alto risco. Por exemplo, você está designado para analisar descobertas ou alertas descobertos por serviços como Amazon GuardDuty e Amazon Inspector.

Na fase de triagem, você determina se acredita que a atividade é realmente positiva (atividade maliciosa genuína) ou falsamente positiva (atividade não maliciosa ou de alto risco). Os perfis do Detective oferecem suporte ao processo de triagem, fornecendo informações sobre a atividade da entidade envolvida.

Para casos verdadeiramente positivos, você continua na próxima fase.

Definição do escopo

Durante a fase de definição do escopo, os analistas determinam a extensão da atividade maliciosa ou de alto risco e a causa subjacente.

A definição do escopo responde aos seguintes tipos de perguntas:

- Quais sistemas e usuários foram comprometidos?
- De onde o ataque se originou?
- Há quanto tempo o ataque está acontecendo?
- Há outra atividade relacionada a ser descoberta? Por exemplo, se um invasor estiver extraindo dados do seu sistema, como ele os obteve?

As visualizações do Detective podem ajudar você a identificar outras entidades envolvidas ou afetadas.

Resposta

A etapa final é responder ao ataque para interrompê-lo, minimizar os danos e evitar que um ataque semelhante aconteça novamente.

Pontos de partida para uma investigação de Detective

Cada investigação no Detective tem um ponto de partida essencial. Por exemplo, você pode receber uma Amazon GuardDuty ou uma AWS Security Hub descoberta para investigar. Ou você pode se preocupar com atividades incomuns em um endereço IP específico.

Os pontos de partida típicos de uma investigação incluem descobertas detectadas GuardDuty e entidades extraídas dos dados de origem do Detective.

Descobertas detectadas por GuardDuty

GuardDuty usa seus dados de registro para descobrir casos suspeitos de atividades maliciosas ou de alto risco. O Detective fornece recursos que ajudam você a investigar essas descobertas.

Para cada descoberta, o Detective fornece os detalhes da descoberta associada. Detective também mostra as entidades, como endereços IP e AWS contas, que estão conectadas à descoberta.

Em seguida, você pode explorar a atividade das entidades envolvidas para determinar se a atividade detectada na descoberta é um motivo genuíno de preocupação.

Para ter mais informações, consulte [the section called “Visão geral da descoberta”](#).

AWS descobertas de segurança agregadas pelo Security Hub

AWS Security Hub agrega descobertas de segurança de vários provedores de descobertas em um único local e fornece uma visão abrangente do seu estado de segurança em AWS. O Security Hub elimina a complexidade de abordar grandes volumes de descobertas de vários provedores. Isso reduz o esforço necessário para gerenciar e melhorar a segurança de todas as suas AWS contas, recursos e cargas de trabalho. O Detective fornece recursos que ajudam você a investigar essas descobertas.

Para cada descoberta, o Detective fornece os detalhes da descoberta associada. Detective também mostra as entidades, como endereços IP e AWS contas, que estão conectadas à descoberta.

Para ter mais informações, consulte [the section called “Visão geral da descoberta”](#).

Entidades extraídas dos dados de origem do Detective

Dos dados de origem do Detective ingeridos, o Detective extrai entidades como endereços IP e usuários da AWS. Você pode usar um deles como ponto de partida da investigação.

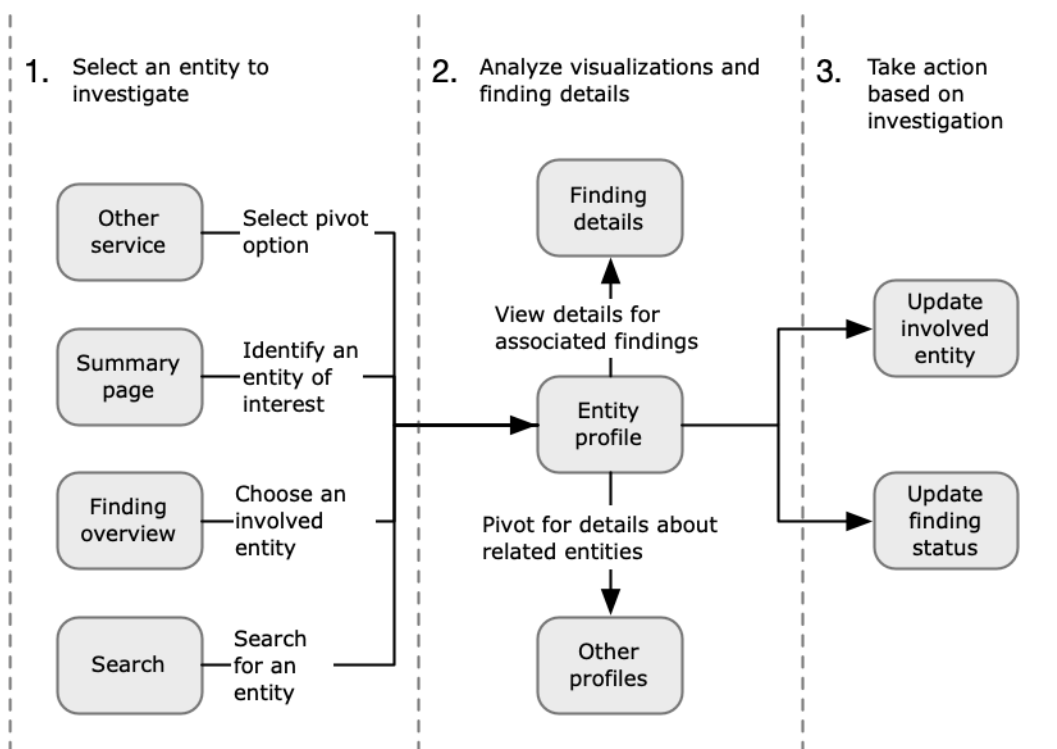
O Detective fornece detalhes gerais sobre a entidade, tais como endereço IP ou nome de usuário. Ele também fornece detalhes sobre o histórico de atividades. Por exemplo, o Detective pode relatar a quais outros endereços IP uma entidade se conectou, foi conectada ou usou.

Para ter mais informações, consulte [Analisando entidades](#).

Fluxo de investigação do Amazon Detective

Você pode usar o Amazon Detective para investigar uma entidade, como uma instância do EC2 ou um usuário. AWS Você também pode investigar as descobertas de segurança.

Em um alto nível, a imagem a seguir mostra o processo de uma Investigação de Detetive.



Etapa 1: selecione a entidade a ser investigada

Ao analisar uma descoberta GuardDuty, os analistas podem optar por investigar uma entidade associada em Detective. Consulte [the section called “Ir a partir de outro console”](#).

Selecionar a entidade leva você ao perfil da entidade no Detective.

Etapa 2: analise as visualizações nos perfis

Cada perfil de entidade contém um conjunto de visualizações que são geradas a partir do gráfico de comportamento. O gráfico de comportamento é criado a partir dos arquivos de log e outros dados que são inseridos no Detective.

As visualizações mostram atividades relacionadas a uma entidade. Você usa essas visualizações para responder perguntas e determinar se a atividade da entidade é incomum. Consulte [Analisando entidades](#).

Para ajudar a orientar a investigação, você pode usar a orientação do Detective fornecida para cada visualização. A orientação descreve as informações exibidas, sugere perguntas para você fazer e propõe as próximas etapas com base nas respostas. Consulte [the section called “Usar a orientação do painel de perfil”](#).

Cada perfil contém uma lista de descobertas associadas. Você pode visualizar os detalhes e a visão geral de uma descoberta. Consulte [the section called “Visualizar descobertas de uma entidade”](#).

A partir de um perfil de entidade, você pode ir para outro perfil de entidade e de descobertas para investigar mais sobre a atividade dos ativos relacionados.

Etapa 3: tome uma medida

Com base nos resultados da sua investigação, tome as medidas apropriadas.

Para uma descoberta que seja um falso positivo, será possível arquivá-la. No Detective, você pode arquivar GuardDuty as descobertas. Consulte [the section called “Arquivando uma descoberta GuardDuty”](#).

Caso contrário, tome as medidas apropriadas para resolver a vulnerabilidade e mitigar os danos. Por exemplo, talvez seja necessário atualizar a configuração de um recurso.

Analizando descobertas no Amazon Detective

Uma descoberta é uma instância de atividade possivelmente maliciosa ou outro risco detectado. As descobertas da Amazon GuardDuty e de AWS segurança são carregadas no Amazon Detective para que você possa usar o Detective para investigar a atividade associada às entidades envolvidas. GuardDuty as descobertas fazem parte do pacote principal do Detective e são ingeridas por padrão. Todas as outras descobertas AWS de segurança agregadas pelo Security Hub são ingeridas como uma fonte de dados opcional. Consulte [Dados de origem usados em um gráfico de comportamento](#) para obter mais detalhes.

A visão geral de uma descoberta do Detective fornece informações detalhadas sobre a descoberta. Também exibe um resumo das entidades envolvidas, com links para os perfis das entidades associadas.

Se uma descoberta estiver relacionada a uma atividade maior, o Detective notifica você a Ir para o grupo da descoberta. Recomendamos usar os grupos da descoberta para continuar sua investigação, pois eles permitem que você examine várias atividades relacionadas a um possível evento de segurança. Consulte [the section called “Encontrando grupos”](#).

Conteúdo

- [Visão geral da análise de uma descoberta](#)
- [Analisar grupos de descobertas](#)
- [Resumo de grupos de descobertas com tecnologia de IA generativa](#)

Visão geral da análise de uma descoberta

A visão geral de uma descoberta do Detective fornece informações detalhadas sobre a descoberta. Também exibe um resumo das entidades envolvidas, com links para os perfis das entidades associadas.

Escopo de tempo usado na visão geral de uma descoberta

O escopo de tempo da visão geral de uma descoberta é definido como a janela de tempo da descoberta. A janela de tempo da descoberta reflete a primeira e a última vez em que a atividade da descoberta foi observada.

Detalhes da descoberta

O painel à direita contém os detalhes da descoberta. Esses são os detalhes fornecidos pelo provedor da descoberta.

A partir dos detalhes da descoberta, você também pode arquivá-la. Consulte [the section called “Arquivando uma descoberta GuardDuty”](#).

Entidades relacionadas

A visão geral de uma descoberta contém uma lista de entidades envolvidas na descoberta. Para cada entidade, a lista fornece informações gerais sobre ela. Essas informações refletem aquelas no painel de perfil de detalhes da entidade no perfil da entidade correspondente.

É possível filtrar a lista com base no tipo de entidade. Também é possível filtrar com base no texto do identificador da entidade.

Para ir para o perfil de uma entidade, escolha Ver perfil. Ao ir para o perfil da entidade, ocorre o seguinte:

- O escopo de tempo é definido como a janela de tempo da descoberta.
- No painel Descobertas associadas da entidade, a descoberta é selecionada. Os detalhes da descoberta continuam sendo exibidos à direita do perfil da entidade.

Solução de problemas de “Página não encontrada”

Ao navegar até uma entidade ou descoberta no Detective, você pode ver uma mensagem de erro Página não encontrada.

Para resolver isso, execute um dos seguintes procedimentos:

- Garanta que a entidade ou descoberta pertença a uma de suas contas-membro. Para obter informações sobre como revisar as contas dos membros, consulte [Visualização da lista de contas](#).
- Certifique-se de que sua conta de administrador esteja alinhada com GuardDuty e/ou com o Security Hub para passar para Detective a partir desses serviços. Para obter as recomendações, consulte [Alinhamento recomendado com o Security Hub GuardDuty e o Security Hub](#).
- Verifique se a descoberta ocorreu depois que a conta-membro aceitou o convite.

- Verifique se o gráfico de comportamento do Detective está ingerindo dados de um pacote de fonte de dados opcional. Para obter mais informações sobre os dados de origem usados nos gráficos de comportamento do Detective, consulte [Dados de origem usados em um](#) gráfico de comportamento.
- Para permitir que o Detective consuma dados do Security Hub e adicione esses dados ao seu gráfico de comportamento, você deve habilitar o Detective para descobertas de AWS segurança como um pacote de fonte de dados. Para obter mais informações, consulte as [descobertas AWS de segurança](#).
- Se você estiver navegando até um perfil de entidade ou uma visão geral de uma descoberta no Detective, garanta que o URL esteja no formato correto. Para obter detalhes sobre a formação de um URL de perfil, consulte [Navegar até o perfil de uma entidade ou até a visão geral de uma descoberta usando um URL](#).

Analisar grupos de descobertas

Os grupos de descobertas do Amazon Detective permitem que você examine várias atividades relacionadas a um possível evento de segurança. Você pode analisar a causa raiz das GuardDuty descobertas de alta severidade usando grupos de localização. Se um agente de ameaças está tentando comprometer seu AWS ambiente, ele normalmente executa uma sequência de ações que levam a várias descobertas de segurança e comportamentos incomuns. Essas ações geralmente estão espalhadas em diferentes períodos e entidades. Quando as descobertas de segurança são investigadas isoladamente, isso pode levar a uma interpretação errônea de sua importância e dificuldade em encontrar a causa raiz. O Amazon Detective resolve esse problema ao aplicar uma técnica de análise gráfica que infere relacionamentos entre descobertas e entidades e as agrupa. Recomendamos tratar os grupos de descobertas como ponto de partida para investigar as entidades e descobertas envolvidas.

O Detective analisa os dados das descobertas e os agrupa com outras descobertas que provavelmente estão relacionadas com base nos recursos que compartilham. Por exemplo, é muito provável que descobertas relacionadas a ações realizadas pelas mesmas sessões de perfil do IAM ou originadas do mesmo endereço IP façam parte da mesma atividade subjacente. É valioso investigar descobertas e evidências em grupo, mesmo que as associações feitas pelo Detective não estejam relacionadas.

Além das descobertas, cada grupo inclui entidades envolvidas nas descobertas. As entidades podem incluir recursos externos AWS , como endereços IP ou agentes de usuário.

Note

Depois que ocorre uma GuardDuty descoberta inicial relacionada a outra descoberta, o grupo de descoberta com todas as descobertas relacionadas e todas as entidades envolvidas é criado em 48 horas.

Entender a página de grupos de descobertas

A página de grupos de descobertas lista todos os grupos de descobertas coletados pelo Amazon Detective a partir de seu gráfico de comportamento. Preste atenção aos seguintes atributos dos grupos de descobertas:

Gravidade de um grupo

Cada grupo de descoberta recebe uma severidade com base na severidade do Formato de Descoberta de AWS Segurança (ASFF) das descobertas associadas. Os valores de severidade de descobertas do ASFF são Crítica, Alta, Média, Baixa ou Informativo, do mais ao menos severo. A severidade de um agrupamento é igual à da descoberta de maior severidade entre as descobertas desse agrupamento.

Grupos que consistem em descobertas de severidade Crítica ou Alta que afetam um grande número de entidades devem ser priorizados nas investigações, pois têm maior probabilidade de representar problemas de segurança de alto impacto.

Título do grupo

Na coluna Título, cada grupo tem um ID exclusivo e um título não exclusivo. Eles se baseiam no namespace do tipo do ASFF para o grupo e no número de descobertas dentro desse namespace no cluster. Por exemplo, se um agrupamento tiver o título: Grupo com: TTP (2), Efeito (1) e Comportamento incomum (2), ele incluirá cinco descobertas no total, consistindo em duas descobertas no namespace TTP, uma no namespace Effect e duas no namespace Unusual Behavior. Para obter uma lista completa de namespaces, consulte [Taxonomia de tipos do ASFF](#).

Táticas em um grupo

A coluna Táticas em um grupo detalha em qual categoria de táticas a atividade se enquadra. As categorias de táticas, técnicas e procedimentos na lista a seguir se alinham à [matriz MITRE ATT&CK](#).

Você pode selecionar uma tática na cadeia para ver uma descrição da tática. Seguindo a cadeia, há uma lista das táticas detectadas no grupo. Essas categorias e as atividades que elas normalmente representam são as seguintes:

- Acesso inicial: um adversário está tentando entrar na rede de outra pessoa.
- Execução: um adversário está tentando entrar na rede de outra pessoa.
- Persistência: um adversário está tentando se manter firme.
- Escalonamento de privilégios: um adversário está tentando obter permissões de nível superior.
- Evasão de defesa: um adversário está tentando evitar ser detectado.
- Acesso credencial: um adversário está tentando roubar nomes e senhas de contas.
- Descoberta: um adversário está tentando entender e aprender sobre um ambiente.
- Movimento lateral: um adversário está tentando se mover em um ambiente.
- Coleta: um adversário está tentando coletar dados que interessam ao seu objetivo.
- Comando e controle: um adversário está tentando entrar na rede de outra pessoa.
- Exfiltração: um adversário está tentando roubar dados.
- Impacto: um adversário está tentando manipular, interromper ou destruir seus sistemas e dados.
- Outra: indica a atividade de uma descoberta que não se alinha às táticas listadas na matriz.

Entidades dentro de um grupo

A coluna Entidades contém detalhes sobre entidades específicas detectadas nesse agrupamento. Selecione esse valor para obter um detalhamento das entidades com base nas categorias: Identidade, Rede, Armazenamento e Computação. Os exemplos de entidades em cada categoria são:

- Identidade — princípios do IAM e Contas da AWS, como usuário e função
- Rede: endereço IP ou outras entidades de rede e VPC
- Armazenamento: buckets do Amazon S3 ou DDBs
- Computação: instâncias do Amazon EC2 ou contêineres do Kubernetes

Contas dentro de um grupo

A coluna Contas informa quais AWS contas possuem entidades envolvidas com as descobertas no grupo. As AWS contas são listadas por nome e AWS ID para que você possa priorizar as investigações de atividades envolvendo contas críticas.

Descobertas dentro de um grupo

A coluna Descobertas lista as entidades dentro de um grupo por severidade. As descobertas incluem descobertas da Amazon, GuardDuty descobertas do Amazon Inspector, descobertas AWS de segurança e evidências do Detective. Você pode selecionar o gráfico para ver uma contagem exata das descobertas por severidade.

GuardDuty as descobertas fazem parte do pacote principal do Detective e são ingeridas por padrão. Todas as outras descobertas AWS de segurança agregadas pelo Security Hub são ingeridas como uma fonte de dados opcional. Consulte [Dados de origem usados em um gráfico de comportamento](#) para obter mais detalhes.

Descobertas informativas em grupos de descobertas

O Amazon Detective identifica informações adicionais relacionadas a um grupo de descobertas com base em dados em seu gráfico de comportamento coletados nos últimos 45 dias. O Detective apresenta essas informações como uma descoberta com a severidade de grau Informativo. Uma evidência fornece informações de apoio que destacam uma atividade incomum ou um comportamento desconhecido que é potencialmente suspeito quando visto em um grupo de descobertas. Isso pode incluir geolocalizações recém-observadas ou chamadas de API observadas dentro do escopo de tempo de uma descoberta. As descobertas de evidências só podem ser visualizadas no Detective e não são enviadas para AWS Security Hub.

Detective determina a localização das solicitações usando bancos de dados GeolIP MaxMind . MaxMind relata uma precisão muito alta de seus dados em nível de país, embora a precisão varie de acordo com fatores como país e tipo de IP. Para obter mais informações sobre MaxMind, consulte [Geolocalização MaxMind IP. Se achar que algum dado do GeolIP está incorreto, você pode enviar uma solicitação de correção para a Maxmind em MaxMind Correct GeolIP2 Data.](#)

Você pode observar evidências de diferentes tipos de entidades principais (tais como usuário do IAM ou perfil do IAM). Para alguns tipos de evidência, você pode observar evidências para todas as contas. Isso significa que as evidências afetam todo o gráfico de comportamento. Se a evidência de uma descoberta for observada em todas as contas, você também verá pelo menos uma evidência

de descoberta informativa adicional do mesmo tipo para um perfil individual do IAM. Por exemplo, se você ver a descoberta Nova geolocalização observada para todas as contas, você verá outra para Nova geolocalização observada para uma entidade principal.

Tipos de evidências em grupos de descobertas

- Nova geolocalização observada
- Nova Organização do Sistema Autônomo (ASO) observada
- Novo agente de usuário observado
- Nova chamada de API emitida
- Nova geolocalização observada para todas as contas
- Nova entidade principal do IAM observada para todas as contas

Perfis de grupos de descobertas

Ao selecionar o título de um grupo, um perfil de grupo de descobertas é aberto com detalhes adicionais sobre esse grupo. O painel de detalhes na página do perfil do grupo de descobertas comporta a exibição de até 1000 entidades e descobertas para grupos de descobertas principais e secundários.

A página do perfil do grupo exibe o Escopo de tempo definido do grupo. Essa é a data e a hora desde a primeira descoberta ou evidência incluída no grupo até a descoberta ou evidência atualizada mais recentemente em um grupo. Você também pode ver a Severidade do grupo de descobertas, que é igual à categoria de maior gravidade entre as descobertas desse grupo. Outros detalhes desse painel de perfil incluem:

- A cadeia de Táticas envolvidas mostra quais táticas são atribuídas às descobertas do grupo. As táticas são baseadas na matriz [MITRE ATT&CK Matrix for Enterprise](#). As táticas são mostradas como uma cadeia de pontos coloridos que representa a progressão típica de um ataque desde o estágio inicial até o mais recente. Isso significa que os círculos mais à esquerda da cadeia normalmente representam atividades menos severas, em que um adversário está tentando obter ou manter o acesso ao seu ambiente. Por outro lado, as atividades à direita são as mais severas e podem incluir adulteração ou destruição de dados.
- Os relacionamentos que esse grupo tem com outros grupos. Ocasionalmente, um ou mais grupos de descobertas anteriormente desconectados podem ser mesclados em um novo grupo com base em um link recém-descoberto, por exemplo, uma descoberta que envolve entidades dos grupos existentes. Nesse caso, o Amazon Detective desativa os grupos principais e cria um grupo

secundário. Você pode rastrear a linhagem de qualquer grupo até seus grupos principais. Os grupos podem ter os seguintes relacionamentos:

- Grupo de descobertas secundário: um grupo de descobertas criado quando uma descoberta envolvida em dois outros grupos de descobertas está envolvida em uma nova descoberta. Os grupos de descobertas principais são listados para qualquer grupo secundário.
- Grupo de descobertas principais: um grupo de descobertas é o principal quando um grupo secundário é criado a partir dele. Se um grupo de descobertas for o principal, os grupos secundários relacionados serão listados com ele. O status de um grupo principal se torna Inativo quando ele é mesclado a um grupo secundário Ativo.

Há duas guias de informação que abrem painéis de perfil. Com as guias Entidades envolvidas e Descobertas envolvidas, você pode visualizar mais detalhes sobre o grupo.

Use Executar investigação para gerar um relatório de investigação. O relatório gerado detalha o comportamento anômalo que indica comprometimento.

Painéis de perfil dentro de grupos

Entidades envolvidas

Concentra-se nas entidades do grupo de descobertas, incluindo a quais descobertas dentro do grupo cada entidade está vinculada. As tags anexadas a cada entidade também são exibidas para que você possa identificar rapidamente as entidades importantes com base nas tags. Selecione uma entidade para ver seu perfil.

Descobertas envolvidas

Tem detalhes sobre cada descoberta, incluindo a severidade da descoberta, cada entidade envolvida e quando essa descoberta foi vista pela primeira e pela última vez. Selecione um tipo de descoberta na lista para abrir um painel de detalhes da descoberta com informações adicionais sobre ela. Como parte do painel de Descobertas envolvidas, você pode ver descobertas com grau Informativo com base nas evidências do Detective no gráfico de comportamento.

Visualização do grupo de descobertas

O Amazon Detective fornece uma visualização interativa dos grupos de descobertas. Essa visualização foi projetada para ajudar você a investigar problemas de modo mais rápido e completo

com menos esforço. O painel de Visualização do grupo de descobertas exibe as descobertas e entidades envolvidas em um grupo de descobertas. Você pode usar essa visualização interativa para analisar, entender e fazer a triagem do impacto do grupo de descobertas. Esse painel ajuda a visualizar as informações apresentadas nas tabelas Entidades envolvidas e Descobertas envolvidas. Na apresentação visual, você pode selecionar descobertas ou entidades para uma análise mais detalhada.

Grupos de descobertas do Detective com descobertas agregadas são um cluster de descobertas conectadas ao mesmo tipo de recurso. Com as descobertas agregadas, você pode avaliar rapidamente a composição de um grupo de descobertas e interpretar os problemas de segurança com mais rapidez. No painel de detalhes dos grupos de descobertas, descobertas semelhantes são combinadas e você pode expandi-las para visualizar descobertas relativamente semelhantes em conjunto. Por exemplo, um nó de evidências, em que descobertas informativas e de severidade média do mesmo tipo são agregadas. Atualmente, você pode visualizar o título, a fonte, o tipo e a severidade dos grupos de descobertas com descobertas agregadas.

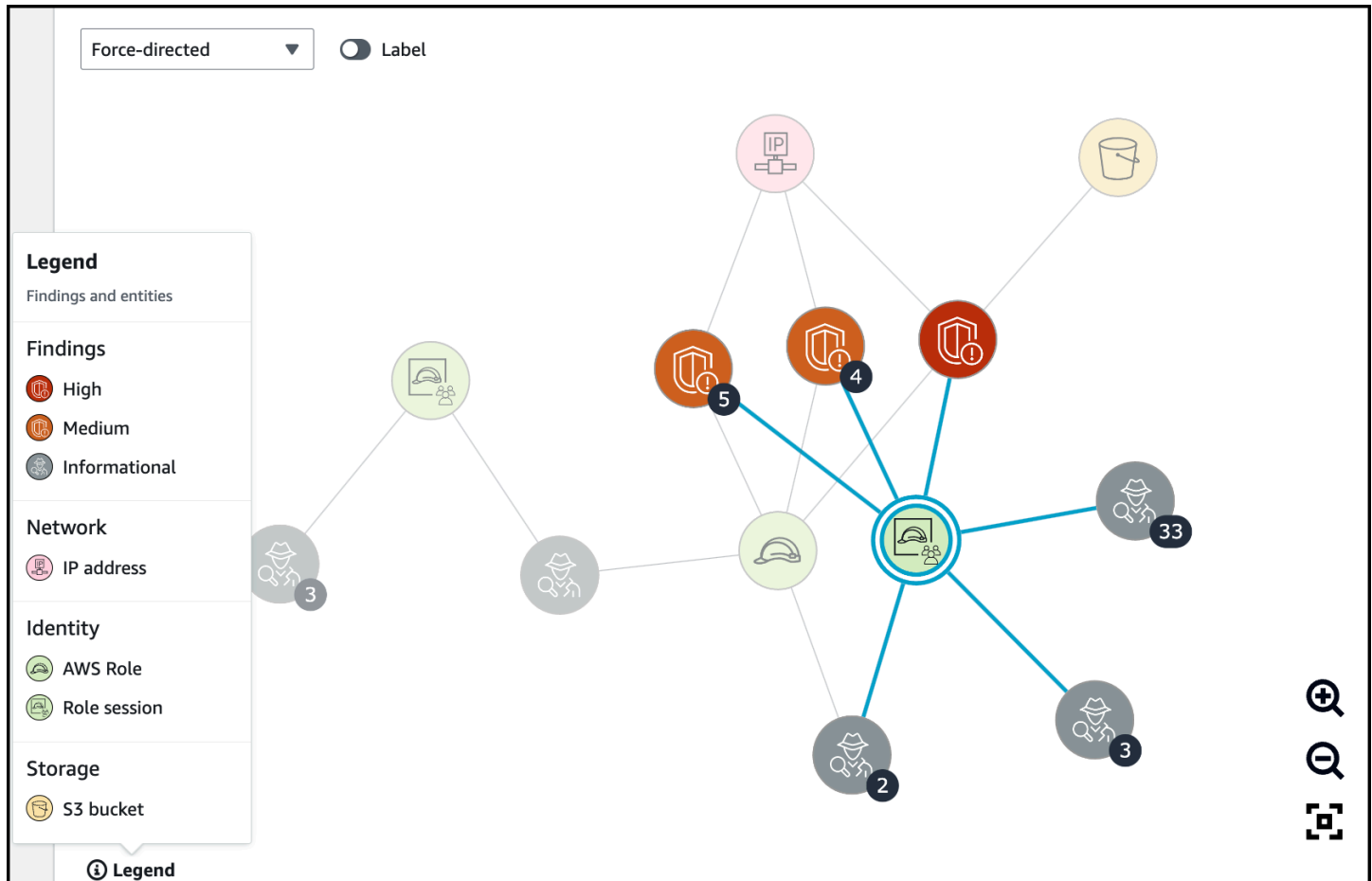
Nesse painel interativo, você pode:

- Use Executar investigação para gerar um relatório de investigação. O relatório gerado detalha o comportamento anômalo que indica comprometimento.
- Visualizar mais detalhes sobre grupos com descobertas agregadas para analisar as evidências, entidades e descobertas envolvidas.
- Visualizar rótulos das entidades e descobertas para identificar as entidades afetadas com possíveis problemas de segurança. Você pode desabilitar a opção Rótulo.
- Reorganizar as entidades e as descobertas para entender melhor sua interconexão. Isolar entidades e descobertas de um grupo ao mover o item selecionado no grupo de descobertas.
- Selecionar as evidências, entidades e descobertas para visualizar mais detalhes sobre elas. Para selecionar vários itens, selecione **command/control** e selecione os itens ou arraste-os e solte-os usando o ponteiro do mouse.
- Ajustar o layout para todas as entidades e descobertas caberem na janela do grupo de descobertas. Visualizar quais tipos de entidade são predominantes em um grupo de descobertas.

Note

O painel de Visualização do grupo de descobertas comporta a exibição de grupos com até 100 entidades e descobertas.

Você pode escolher **Selecionar layout** para visualizar as descobertas e entidades em um layout Circular, Direcionado por força ou Em grade. O layout Direcionado por força posiciona as entidades e descobertas de modo que os links tenham um comprimento consistente entre os itens e que sejam distribuídos uniformemente. Isso ajuda a reduzir a sobreposição. O layout selecionado define o posicionamento das descobertas no painel de Visualização.



A Legenda dinâmica muda com base nas entidades e descobertas em seu gráfico atual. Ela ajuda você a identificar o que cada elemento visual representa.

Resumo de grupos de descobertas com tecnologia de IA generativa

Por padrão, o Amazon Detective automaticamente fornece resumos de um grupo de descobertas individual. Os resumos são alimentados por modelos inteligência artificial generativa (IA generativa) hospedados no [Amazon Bedrock](#).

Ao usar grupos de descobertas, você pode examinar várias descobertas de segurança, visto que elas se relacionam a um possível evento de segurança, e identificar possíveis agentes de ameaças. Os resumos de grupo de descobertas para grupos de descobertas se baseiam nesses recursos. Os resumos de grupo de descobertas consomem os dados de um grupo de descobertas, rapidamente analisam as relações entre as descobertas e os recursos afetados e resume as possíveis ameaças em linguagem natural. Você pode aproveitar esses resumos para identificar ameaças maiores à segurança, melhorar a eficiência da investigação e reduzir os prazos de resposta.

Note

Os resumos de grupos de descobertas baseados em IA generativa podem, nem sempre, fornecer informações totalmente precisas. Para obter mais informações, consulte [Política de uso responsável de IA da AWS](#).

Analisar o resumo de grupos de descobertas

O resumo de grupos de descobertas de um grupo de descobertas fornece uma explicação clara e detalhada sobre um evento de segurança. Em linguagem natural, a explicação inclui um título sucinto, um resumo dos recursos envolvidos e informações selecionadas sobre esses recursos.

Como analisar um resumo de grupos de descobertas

1. Abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, selecione Grupos de descobertas.
3. Na tabela Grupos de descobertas, selecione o grupo de descobertas do qual você deseja exibir um resumo. Uma página de detalhes é exibida.

Na página de detalhes, use o painel Resumo para analisar um resumo descritivo gerado das principais descobertas no grupo de descobertas. Você também pode revisar uma análise dos principais eventos de ameaça no grupo de descobertas, que você pode então investigar mais detalhadamente. Selecione o ícone de cópia no painel para adicionar o resumo gerado às suas observações ou a um sistema de emissão de bilhetes. Essa ação copia o resumo para a área de transferência. Você também pode compartilhar seus comentários sobre o resultado do resumo de grupo de descobertas no resumo, o que pode proporcionar uma experiência melhor no futuro. Para compartilhar seus comentários, selecione o ícone de polegar para cima ou para baixo, dependendo da natureza dos seus comentários.

 Note

Se você fizer comentários sobre o resumo de grupo de descobertas, eles não serão usados para ajustar o modelo. Nós usamos esses comentários apenas para ajudar a facilitar que as instruções no Detective sejam elaboradas de forma eficaz.

Summary - *new* Info

Credentials exfiltration from i-0e5f7e596391b28eb using role privilegedRole

Instance i-0e5f7e596391b28eb had newly observed API calls and user agents for role privilegedRole.

Credentials for role privilegedRole on i-0e5f7e596391b28eb were exfiltrated and used from account [REDACTED] and IP [REDACTED].

The exfiltrated credentials were used to access S3 bucket private-bucket-[REDACTED].

i-0e5f7e596391b28eb was vulnerable to CVE-2021-44228 and CVE-2021-45046.



Desabilitar o resumo de grupo de descobertas

Por padrão, o resumo de grupo de descobertas é habilitado para grupos de descobertas. Você pode desabilitar o resumo de grupo de descobertas a qualquer momento. É possível habilitá-lo posteriormente.

Como desativar o resumo de grupo de descobertas

1. Abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, escolha Preferences.
3. Em Resumo de grupo de descobertas, selecione Editar.
4. Desative a opção Habilitado.
5. Escolha Salvar.

Habilitar o resumo de grupo de descobertas

Se você desabilitou o resumo de grupo de descobertas para grupos de descobertas, você poderá habilitá-lo novamente a qualquer momento.

Como habilitar o resumo de grupo de descobertas

1. Abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, escolha Preferences.
3. Em Resumo de grupo de descobertas, selecione Editar.
4. Ative a opção Habilitado.
5. Escolha Salvar.

Regiões compatíveis

O resumo do grupo de busca está disponível nas seguintes AWS regiões.

- Leste dos EUA (Norte da Virgínia)
- Oeste dos EUA (Oregon)
- Ásia-Pacífico (Tóquio)
- Europa (Frankfurt)

Análise de entidades no Amazon Detective

Uma entidade é um único objeto extraído dos dados de origem. Os exemplos incluem um endereço IP específico, uma instância do Amazon EC2 ou AWS uma conta. Consulte [the section called “Tipos de entidades na estrutura de dados do gráfico de comportamento”](#) para obter uma lista dos tipos de entidade.

Um perfil de entidade do Amazon Detective é uma página única que fornece informações detalhadas sobre a entidade e sua atividade. Você pode usar um perfil de entidade para obter detalhes de apoio a uma investigação sobre uma descoberta ou como parte de uma busca geral por atividades suspeitas.

Conteúdo

- [Usar a página Resumo para identificar uma entidade de interesse](#)
- [Usando perfis de entidade](#)
- [Visualizar e interagir com painéis de perfil](#)
- [Navegar diretamente até o perfil de uma entidade ou até a visão geral de uma descoberta](#)
- [Navegar por um perfil](#)
- [Gerenciar o escopo de tempo](#)
- [Visualizar detalhes das descobertas associadas](#)
- [Visualizar detalhes de entidades de alto volume](#)

Usar a página Resumo para identificar uma entidade de interesse

Use a página Resumo no Amazon Detective para identificar entidades cuja origem da atividade nas últimas 24 horas deve ser investigada. A página Resumo do Amazon Detective ajuda você a identificar entidades que estão associadas a tipos específicos de atividades incomuns. É um dos vários pontos de partida possíveis para uma investigação.

Para exibir a página Resumo, no painel de navegação do Detective, escolha Resumo. A página Resumo também é exibida por padrão ao abrir o console do Detective pela primeira vez.

Na página Resumo, você pode identificar entidades que atendem aos seguintes critérios:

- Investigações que revelam possíveis eventos de segurança identificados pelo Detective
- Entidades envolvidas em atividades que ocorreram em geolocalizações recém-observadas

- Entidades que fizeram o maior número de chamadas de API
- Instâncias do EC2 que tiveram o maior volume de tráfego
- Clusters de contêiner que tiveram o maior número de contêineres

No painel de cada página de Resumo, você pode ir até o perfil de uma entidade selecionada.

Ao revisar a página Resumo, você pode ajustar o Escopo de tempo para visualizar a atividade em qualquer período de 24 horas nos últimos 365 dias. Ao alterar a Data e hora de início, a Data e hora de término é atualizada automaticamente para 24 horas após a hora de início escolhida.

Com o Detective, você pode acessar até um ano de dados do histórico de eventos. Esses dados estão disponíveis por meio de um conjunto de visualizações que mostram mudanças no tipo e volume de atividade em uma janela de tempo selecionada. Detective vincula essas mudanças às GuardDuty descobertas.

Para obter mais informações sobre os dados de origem no Detective, consulte [Dados de origem usados em um gráfico de comportamento](#).

Investigações

O painel Investigações revela os possíveis eventos de segurança identificados pelo Detective. No painel Investigações, você pode ver investigações Críticas e os perfis e usuários da AWS correspondentes que foram afetados por eventos de segurança em um determinado período. As investigações agrupam indicadores de comprometimento para ajudar a determinar se um AWS recurso está envolvido em atividades incomuns que podem indicar comportamento malicioso e seu impacto.

Selecione **Veja todas as investigações** para analisar as descobertas, os grupos de descobertas de triagem e os detalhes dos recursos para acelerar a investigação de segurança. As investigações são exibidas com base no Tempo de escopo selecionado. Você pode ajustar o tempo de escopo para visualizar as investigações de um período de 24 horas dos últimos 365 dias. Acesse **Investigações críticas** diretamente para ver um relatório detalhado de investigação.

Se você identificar uma AWS função ou usuário que parece ter atividade suspeita, você pode ir diretamente do painel Investigações para a função ou usuário para continuar sua investigação. Vá para um perfil ou usuário e clique em **Executar investigação** para gerar um relatório de investigação. Depois de realizar uma investigação sobre um perfil ou usuário, ele é movido para a guia **Investigado**.

Geolocalizações recém-observadas

Geolocalizações recém-observadas destacam as localizações geográficas que originaram a atividade nas 24 horas anteriores, mas que não foram vistas durante o período básico anterior.

O painel inclui até 100 geolocalizações. As localizações estão marcadas no mapa e listadas na tabela abaixo do mapa.

Para cada geolocalização, a tabela exibe o número de chamadas de API malsucedidas e bem-sucedidas feitas a partir dessa geolocalização nas últimas 24 horas.

Você pode expandir cada geolocalização para exibir a lista de usuários e funções que fizeram chamadas de API a partir dessa geolocalização. Para cada entidade principal, a tabela lista o tipo e a Conta da AWS associada.

Se você identificar um usuário ou função que pareça suspeito, poderá ir diretamente do painel para o perfil do usuário ou da função para continuar sua investigação. Para ir até um perfil, escolha o identificador do usuário ou da função.

Detective determina a localização das solicitações usando bancos de dados GeolIP MaxMind . MaxMind relata uma precisão muito alta de seus dados em nível de país, embora a precisão varie de acordo com fatores como país e tipo de IP. Para obter mais informações sobre MaxMind, consulte [Geolocalização MaxMind IP](#). [Se achar que algum dado do GeolIP está incorreto, você pode enviar uma solicitação de correção para a Maxmind em MaxMind Correct GeolIP2 Data](#).

Grupos de descobertas ativos nos últimos 7 dias

Grupos de descobertas ativos nos últimos 7 dias mostra grupos correlacionados de descobertas do Detective, entidades e evidências em seu ambiente que ocorreram em um determinado período. Esses grupos correlacionam atividades incomuns que podem indicar comportamento malicioso. A página Resumo mostra até cinco grupos, classificados pelos grupos contendo as descobertas mais críticas que estiveram ativas na última semana.

Você pode selecionar valores no conteúdo Tática, Conta, Recurso e Descobertas para ver mais detalhes.

Grupos de descobertas são gerados diariamente. Se você identificar um grupo de descobertas interessante, poderá selecionar o título para acessar uma visualização detalhada do perfil de um grupo e continuar sua investigação.

Funções e usuários com o maior volume de chamadas de API

Funções e usuários com o maior volume de chamadas de API identifica os usuários e funções que fizeram o maior número de chamadas de API nas últimas 24 horas.

O painel pode incluir até 100 usuários e funções. Para cada usuário ou função, você pode ver o tipo (usuário ou função) e a conta associada. Você também pode ver o número de chamadas de API emitidas por esse usuário ou função nas últimas 24 horas.

Por padrão, as funções vinculadas a serviços são exibidas. As funções vinculadas a serviços podem produzir grandes volumes de AWS CloudTrail atividade, o que substitui os principais que você deseja investigar mais detalhadamente. Você pode optar por desativar Mostrar funções vinculadas ao serviço para filtrar as funções vinculadas a serviços na visualização da página Resumo.

Você pode exportar um arquivo de valores separados por vírgula (.csv) que contém os dados desse painel.

Também há um cronograma do volume de chamadas de API nos últimos 7 dias. O cronograma pode ajudar você a determinar se o volume de chamadas de API é incomum para essa entidade principal.

Se você identificar um usuário ou função cujo volume de chamadas de API pareça suspeito, poderá ir diretamente do painel para o perfil do usuário ou da função para continuar sua investigação. Você também pode visualizar o perfil da conta associada ao usuário ou à função. Para visualizar um perfil, escolha o identificador do usuário, da função ou da conta.

Instâncias do EC2 com o maior volume de tráfego

Instâncias do EC2 com o maior volume de tráfego identifica as instâncias do EC2 que tiveram o maior volume total de tráfego nas últimas 24 horas.

O painel pode incluir até 100 instâncias do EC2. Para cada instância do EC2, você pode ver a conta associada e o número de bytes de entrada, bytes de saída e o total de bytes das últimas 24 horas.

É possível exportar um arquivo .csv (valores separados por vírgula) contendo os dados nesse painel.

Você também pode ver um cronograma mostrando o tráfego de entrada e saída nos últimos 7 dias. O cronograma pode ajudar a determinar se o volume de tráfego é incomum para essa instância do EC2.

Se você identificar uma instância do EC2 com volume de tráfego suspeito, poderá ir diretamente do painel para o perfil da instância do EC2 para continuar sua investigação. Você também pode

visualizar o perfil da conta proprietária da instância do EC2. Para visualizar um perfil, escolha o identificador da instância do EC2 ou da conta.

Clusters de contêiner com o maior número de pods do Kubernetes

Clusters de contêiner com o maior número de pods do Kubernetes criados identifica os clusters que tiveram mais contêineres em execução nas últimas 24 horas.

Esse painel inclui até 100 clusters organizados por quais clusters tiveram mais descobertas associadas a eles. Para cada cluster, você pode ver a conta associada, o número atual de contêineres nesse cluster e o número de descobertas associadas a esse cluster nas últimas 24 horas. É possível exportar um arquivo .csv (valores separados por vírgula) contendo os dados nesse painel.

Se você identificar um cluster com descobertas recentes, poderá ir diretamente do painel para o perfil do cluster para continuar sua investigação. Você também pode ir até o perfil da conta proprietária do cluster. Para ir até um perfil, escolha o nome do cluster ou o identificador da conta.

Notificação de valor aproximado

Em Funções e usuários com o maior volume de chamadas de API e Instâncias do EC2 com o maior volume de tráfego, se um valor for seguido por um asterisco (*), isso significa que o valor é uma aproximação. O valor verdadeiro é igual ou maior que o valor exibido.

Isso ocorre devido ao método que o Detective usa para calcular o volume para cada intervalo de tempo. Na página Resumo, o intervalo de tempo é de uma hora.

Para cada hora, o Detective calcula o volume total para os 1.000 usuários, funções ou instâncias do EC2 com o maior volume. Ela exclui os dados dos demais usuários, funções ou instâncias do EC2.

Se um recurso às vezes estava entre os 1.000 primeiros e às vezes não, o volume calculado para esse recurso pode não incluir todos os dados. Os dados dos intervalos de tempo em que não estava entre os 1.000 primeiros são excluídos.

Observe que isso se aplica apenas à página Resumo. O perfil do usuário, da função ou da instância do EC2 fornece detalhes precisos.

Usando perfis de entidade

Um perfil de entidade aparece quando você executa uma das seguintes ações:

- No GuardDuty console da Amazon, escolha a opção de investigar uma entidade relacionada a uma descoberta selecionada.

Consulte [the section called “Ir a partir de outro console”](#).

- Acesse o URL do Detective para ver o perfil da entidade.

Consulte [the section called “Navegar usando um URL”](#).

- Use a pesquisa do Detective no console para pesquisar uma entidade.
- Escolha um link para o perfil da entidade a partir de outro perfil de entidade ou da visão geral de uma descoberta.

Escopo de tempo de um perfil de entidade

Quando você navega diretamente para um perfil de entidade sem fornecer o escopo de tempo, o escopo de tempo é definido para as 24 horas anteriores.

Quando você navega para um perfil de entidade a partir de outro perfil de entidade, o escopo de tempo atualmente selecionado permanece em vigor.

Quando você navega para um perfil de entidade a partir da visão geral de uma descoberta, o escopo de tempo é definido como a janela de tempo da descoberta.

Para obter informações sobre como personalizar o tempo do escopo para limitar os dados exibidos nos perfis da entidade, consulte [Gerenciando o tempo do escopo](#).

Identificador e tipo de entidade

Na parte superior do perfil estão o identificador da entidade e o tipo de entidade. Cada tipo de entidade tem um ícone correspondente, para fornecer um indicador visual do tipo de perfil.

Descobertas envolvidas

Cada perfil contém uma lista das descobertas nas quais a entidade esteve envolvida durante o escopo de tempo.

Você pode ver os detalhes de cada descoberta, alterar o escopo de tempo para refletir a janela de tempo da descoberta e acessar a visão geral da descoberta para procurar outros recursos envolvidos.

Consulte [the section called “Visualizar descobertas de uma entidade”](#).

Grupos de descobertas envolvendo essa entidade

Cada perfil contém uma lista de grupos de descobertas nos quais uma entidade está incluída.

O grupo de uma descoberta é composto de descobertas, entidades e evidências que o Detective coleta em um grupo para fornecer mais contexto sobre possíveis problemas de segurança.

Para obter mais informações sobre grupos de descobertas, consulte [the section called “Encontrando grupos”](#).

Painéis de perfil contendo detalhes da entidade e resultados de análises

O perfil de cada entidade contém um conjunto de uma ou mais guias. Cada guia contém um ou mais painéis de perfil. Cada painel de perfil contém texto e visualizações que são gerados a partir dos dados do gráfico de comportamento. As guias e painéis de perfil específicos são personalizados de acordo com o tipo de entidade.

Para a maioria das entidades, o painel na parte superior da primeira guia fornece informações resumidas de alto nível sobre a entidade.

Outros painéis de perfil destacam diferentes tipos de atividade. Para uma entidade envolvida em uma descoberta, as informações nos painéis de perfil da entidade podem fornecer evidências de apoio adicionais para ajudar a concluir uma investigação. Cada painel de perfil fornece acesso a orientações sobre como usar as informações. Para ter mais informações, consulte [the section called “Usar a orientação do painel de perfil”](#).

Para obter mais detalhes sobre os painéis de perfil, os tipos de dados que eles contêm e as opções disponíveis para interagir com eles, consulte [the section called “Visualizar e interagir com painéis de perfil”](#).

Visualizar e interagir com painéis de perfil

Cada perfil de entidade no console do Amazon Detective consiste em um conjunto de painéis de perfil. Um painel de perfil é uma visualização que fornece detalhes gerais ou destaca atividades específicas associadas a uma entidade. Os painéis de perfil usam diferentes tipos de visualizações para apresentar diferentes tipos de informações. Também podem fornecer links para detalhes adicionais ou para outros perfis.

Cada painel de perfil tem como objetivo ajudar os analistas a encontrarem respostas para perguntas específicas sobre entidades e suas atividades associadas. As respostas para essas perguntas ajudam a concluir se a atividade representa uma ameaça genuína.

Conteúdo

- [Conteúdo do painel de perfil](#)
- [Configurar as preferências de um painel de perfil](#)
- [Mudar de um painel de perfil para outro console](#)
- [Mudar de um painel de perfil para outro perfil de entidade](#)
- [Explorar detalhes da atividade em um painel de perfil](#)

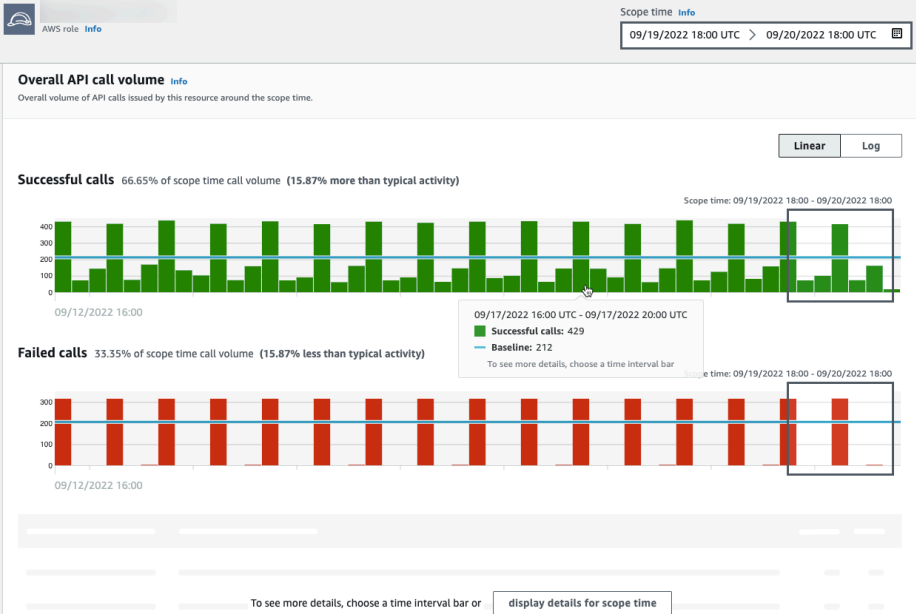
Conteúdo do painel de perfil

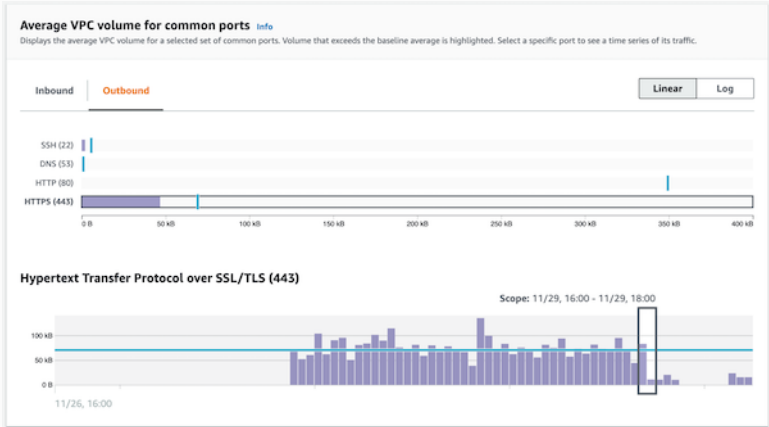
Os painéis de perfil usam diferentes tipos de visualizações para apresentar diferentes tipos de informações.

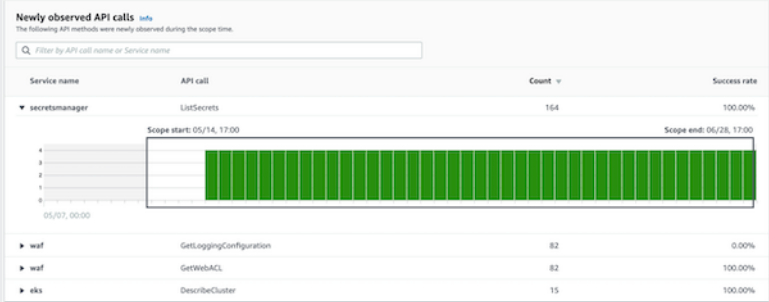
Tipos de informações em um painel de perfil

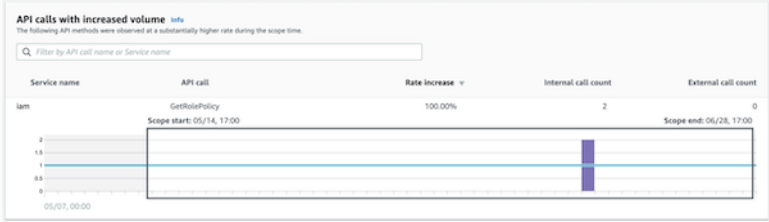
Os painéis de perfil geralmente fornecem os seguintes tipos de dados.

Tipo de dados do painel	Descrição
<p>Informações de alto nível sobre uma descoberta ou entidade</p>	<p>O tipo de painel mais simples fornece algumas informações básicas sobre uma entidade.</p> <p>Exemplos de informações incluídas em um painel de informações incluem o identificador, nome, tipo e data de criação.</p> <div data-bbox="591 1486 1507 1728" data-label="Image"> </div> <p>A maioria dos perfis de entidade contém um painel de informações para essa entidade.</p>

Tipo de dados do painel	Descrição
Resumo geral da atividade ao longo do tempo	<p>Exibe um resumo da atividade de uma entidade ao longo do tempo.</p> <p>Esse tipo de painel fornece uma visão geral de como uma entidade está se comportando durante o escopo de tempo.</p>  <p>Veja a seguir alguns exemplos de dados de resumo fornecidos nos painéis de perfis do Detective:</p> <ul style="list-style-type: none"> • Chamadas de API malsucedidas e bem-sucedidas • Volume de entrada e saída do VPC

Tipo de dados do painel	Descrição
Resumo da atividade agrupado por valores	<p>Exibe um resumo da atividade de uma entidade, agrupado por valores específicos.</p> <p>Você pode ver esse tipo de painel de perfil no perfil de uma instância do EC2. O painel de perfil mostra o volume médio de dados de log de fluxo do VPC de e para uma instância do EC2 para portas comuns associadas a tipos específicos de serviços.</p>  <p>The screenshot displays two charts. The top chart, titled 'Average VPC volume for common ports', shows the average volume for four ports: SSH (22), DNS (53), HTTP (80), and HTTPS (443). The x-axis represents volume in kB, ranging from 0 to 400. The bottom chart, titled 'Hypertext Transfer Protocol over SSL/TLS (443)', shows a time series of traffic volume from 11/26, 16:00 to 11/29, 18:00. A red box highlights a peak in traffic volume around 11/29, 18:00.</p>

Tipo de dados do painel	Descrição
Atividade que só começou durante o escopo de tempo	<p>Durante uma investigação, é importante ver quais atividades só começaram a ocorrer durante um período específico.</p> <p>Por exemplo, há chamadas de API, localizações geográficas ou agentes de usuário que não foram vistos antes?</p>  <p>Se o gráfico de comportamento ainda estiver no modo de treinamento, o painel de perfil exibirá uma mensagem de notificação. A mensagem é removida quando o gráfico de comportamento acumula pelo menos duas semanas de dados. Para mais informações sobre o modo de treinamento, consulte the section called “Período de treinamento para novos gráficos de comportamento”.</p>

Tipo de dados do painel	Descrição
<p>Atividade que mudou significativamente durante o escopo de tempo</p>	<p>Semelhante aos novos painéis de atividades, os painéis de perfil também podem exibir atividades que mudaram significativamente durante o escopo de tempo.</p> <p>Por exemplo, um usuário pode emitir regularmente uma determinada chamada de API algumas vezes por semana. Se o mesmo usuário fizer repentinamente a mesma chamada várias vezes em um único dia, isso pode ser evidência de atividade maliciosa.</p>  <p>Se o gráfico de comportamento ainda estiver no modo de treinamento, o painel de perfil exibirá uma mensagem de notificação. A mensagem é removida quando o gráfico de comportamento acumula pelo menos duas semanas de dados. Para mais informações sobre o modo de treinamento, consulte the section called “Período de treinamento para novos gráficos de comportamento”.</p>

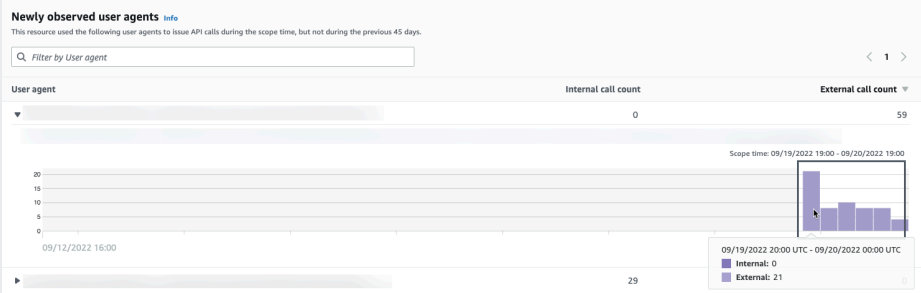
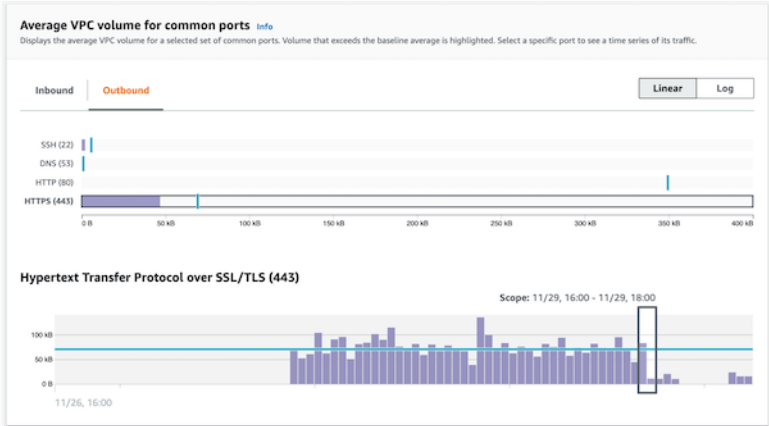
Tipos de visualizações do painel de perfil

O conteúdo do painel do perfil pode assumir uma das formas a seguir.

Tipo de visualização	Descrição
Pares de chave-valor	<p>O tipo de visualização mais simples é um conjunto de pares de chave-valor.</p> <p>Um painel de informações de descobertas ou entidades é o exemplo mais comum de um painel de par de chave-valor.</p>

Tipo de visualização	Descrição															
	<div data-bbox="592 216 1507 453"> <p>Role details Info</p> <table border="1"> <tr> <td>AWS role</td> <td>Principal ID</td> <td>AWS account</td> </tr> <tr> <td>Created by</td> <td>Created date</td> <td>Last observed</td> </tr> <tr> <td>-</td> <td>-</td> <td>09/20/2022 16:46 UTC</td> </tr> <tr> <td>Role description</td> <td></td> <td></td> </tr> <tr> <td>-</td> <td></td> <td></td> </tr> </table> </div> <p>Os pares de chave-valor também podem ser usados para adicionar informações adicionais a outros tipos de painéis.</p> <p>Em um painel de pares de chave-valor, se um valor for um identificador de uma entidade, você poderá ir até o perfil dela.</p>	AWS role	Principal ID	AWS account	Created by	Created date	Last observed	-	-	09/20/2022 16:46 UTC	Role description			-		
AWS role	Principal ID	AWS account														
Created by	Created date	Last observed														
-	-	09/20/2022 16:46 UTC														
Role description																
-																
Tabela	<p>Uma tabela é uma lista simples de itens com várias colunas.</p> <div data-bbox="592 814 1507 968"> <p>Observed IP address assignments based on VPC Flow</p> <p>These IP addresses were assigned to this EC2 instance and also had traffic with the instance</p> <p>Q Filter by IP CIDR</p> <table border="1"> <thead> <tr> <th>IP address</th> <th>First observed</th> <th>Last observed</th> </tr> </thead> <tbody> <tr> <td>10.101.0.119</td> <td>04/27/2021 15:19 UTC</td> <td>09/20/2022 17:45 UTC</td> </tr> </tbody> </table> </div> <p>Você pode classificar, filtrar e percorrer a tabela.</p> <p>Você pode alterar o número de entradas a serem exibidas em cada página. Consulte the section called “Preferências de painéis de perfil”.</p> <p>Se um valor na tabela for um identificador de uma entidade, você poderá ir até o perfil dela.</p>	IP address	First observed	Last observed	10.101.0.119	04/27/2021 15:19 UTC	09/20/2022 17:45 UTC									
IP address	First observed	Last observed														
10.101.0.119	04/27/2021 15:19 UTC	09/20/2022 17:45 UTC														

Tipo de visualização	Descrição
Linha do tempo	<p>Uma visualização do cronograma mostra um valor agregado para intervalos definidos ao longo do tempo.</p>  <p>O cronograma destaca o escopo de tempo atual e inclui um tempo periférico adicional antes e depois do escopo de tempo. O tempo periférico fornece contexto para a atividade no escopo de tempo.</p> <p>Passa o mouse sobre um intervalo de tempo para exibir um resumo dos dados desse intervalo de tempo.</p>

Tipo de visualização	Descrição
Tabela expansível	<p>Uma tabela expansível combina tabelas e cronogramas.</p>  <p>A visualização começa como uma tabela.</p> <p>Você pode classificar, filtrar e percorrer a tabela.</p> <p>Você pode alterar o número de entradas a serem exibidas em cada página. Consulte the section called “Preferências de painéis de perfil”.</p> <p>Em seguida, você pode expandir cada linha para mostrar uma visualização específica do cronograma dessa linha.</p>
Gráfico de barras	<p>Um gráfico de barras mostra valores com base em agrupamentos.</p> <p>Dependendo do gráfico, você pode escolher uma barra para exibir um cronograma de atividades relacionadas.</p> 

Tipo de visualização	Descrição
Gráfico de geolocalização	<p>Um gráfico de geolocalização exibe um mapa marcado para destacar dados com base na localização geográfica. Pode ser seguido por uma tabela contendo detalhes sobre geolocalizações individuais.</p>  <p>Observe que, ao processar dados geográficos recebidos, o Detective arredonda os valores de latitude e longitude para um único ponto decimal.</p>

Outras observações sobre o conteúdo do painel de perfil

Ao visualizar o conteúdo de um painel de perfil, esteja ciente dos seguintes itens:

Aviso de dados de contagem aproximada

Esse aviso indica que itens com contagens extremamente baixas não aparecem devido ao volume de dados aplicáveis.

Para garantir uma contagem totalmente precisa, reduza a quantidade de dados. A maneira mais simples de fazer isso é reduzir a duração do escopo de tempo. Consulte [the section called “Gerenciar o escopo de tempo”](#).

Arredondamento para localizações geográficas

O Detective arredonda todos os valores de latitude e longitude para um único ponto decimal.

Mudanças na forma como o Detective representa as chamadas de API

A partir de 14 de julho de 2021, o Detective rastreia o serviço que fez cada chamada de API. Sempre que o Detective exibe um método de API, ele também exibe o serviço associado. Nos painéis de perfil que exibem informações sobre chamadas de API, as chamadas são sempre agrupadas pelo serviço. Para dados que o Detective ingeriu antes dessa data, o nome do serviço é listado como Serviço desconhecido.

Também a partir de 14 de julho de 2021, para contas e funções, os detalhes da atividade do painel de perfil Volume geral de chamadas de API não mostram mais o AKID do recurso que emitiu a chamada. Para contas, o Detective exibe o identificador da entidade principal (usuário ou função) que emitiu a chamada. Para funções, o Detective exibe o identificador da sessão de função. Para dados que o Detective ingeriu antes de 14 de julho de 2021, o identificador é listado como Recurso desconhecido.

Para painéis de perfil que exibem uma lista de chamadas de API, o cronograma associado destaca o período durante o qual essa transição ocorreu. O destaque começa em 14 de julho de 2021 e termina quando a atualização foi totalmente propagada no Detective.

Configurar as preferências de um painel de perfil

No console do Detective, você pode definir o Tamanho da tabela e a exibição do Carimbo de data/hora na página Preferências.

Definir o tamanho da tabela

Para painéis de perfil que contêm tabelas ou tabelas expansíveis, você pode configurar o número de linhas a serem exibidas em cada página.

Defina sua preferência para o número de entradas em cada página.

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, em Configurações, selecione Preferências.
3. Na página Preferências, em Tamanho da tabela, clique em Editar.
4. Escolha o número de linhas da tabela que você deseja exibir em cada página.
5. Escolha Salvar.

Definir o formato do carimbo de data/hora

Para painéis de perfil, você pode configurar a preferência de formato do carimbo de data/hora que será aplicada a todos os carimbos de data/hora de cada usuário do IAM ou perfil do IAM no Detective.

Note

A preferência de formato de carimbo de data/hora não é aplicada em toda AWS a conta.

Defina a preferência do carimbo de data/hora.

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, em Configurações, selecione Preferências.
3. Na página Preferências, em Preferências do carimbo de data/hora, visualize e altere a exibição preferida para todos os carimbos de data/hora.
4. Por padrão, o formato do carimbo de data/hora é definido como UTC. Clique em Editar para escolher seu fuso horário local.

Exemplo:

Example

UTC - 20/09/22 16:39 UTC

Local - 20/09/2022 9:39 (UTC-07:00)

5. Escolha Salvar.

Mudar de um painel de perfil para outro console

Para instâncias do EC2, usuários do IAM e perfis do IAM, você pode navegar diretamente do painel de perfil de detalhes até o console correspondente. As informações disponíveis no console podem fornecer informações adicionais para sua investigação.

No painel de perfil Detalhes da instância do EC2, o identificador da instância do EC2 está vinculado ao console do Amazon EC2.

No painel de perfil Detalhes do usuário, o nome do usuário está vinculado ao console do IAM.

No painel de perfil Detalhes da função, o nome da função está vinculado ao console do IAM.

Mudar de um painel de perfil para outro perfil de entidade

Quando um painel de perfil contém um identificador de uma entidade diferente, geralmente é um link para o perfil dessa entidade. As exceções são os links para os consoles do Amazon EC2 e do IAM nos perfis de instâncias do EC2, usuários do IAM e perfis do IAM. Consulte [the section called “Mudar para outro console”](#).

Por exemplo, em uma lista de endereços IP, você pode exibir o perfil de um endereço IP específico. Dessa forma, você pode ver se há alguma outra informação disponível para ajudar a concluir sua investigação.

Explorar detalhes da atividade em um painel de perfil

Durante uma investigação, você pode investigar com mais detalhes o padrão de atividade de uma entidade.

Nos painéis de perfil a seguir, você pode exibir um resumo dos detalhes da atividade:

- Volume geral de chamadas de API, exceto para o painel de perfil no perfil do agente de usuário
- Geolocalizações recém-observadas
- Volume geral de fluxo do VPC
- Volume de fluxo do VPC do e para o endereço IP da descoberta, para descobertas associadas a um único endereço IP
- Detalhes do contêiner
- Volume de fluxo do VPC para clusters
- Atividade geral da API do Kubernetes

Os detalhes da atividade podem responder a estes tipos de perguntas:

- Quais endereços IP foram usados?
- Onde esses endereços IP estavam localizados?
- Quais chamadas de API cada endereço IP fez e de quais serviços eles fizeram essas chamadas?
- Quais entidades principais ou identificadores de chave de acesso (AKIDs) foram usados para fazer as chamadas?

- Quais recursos foram usados para fazer essas chamadas?
- Quantas chamadas foram feitas? Quantas tiveram sucesso e quantas falharam?
- Qual volume de dados de log de fluxo do VPC foi enviado para ou de cada endereço IP?
- Quais contêineres estavam ativos para um determinado cluster, imagem ou pod?

Tópicos

- [Detalhes da atividade para o volume geral de chamadas de API](#)
- [Detalhes da atividade para uma geolocalização](#)
- [Detalhes da atividade para o volume geral de fluxo do VPC](#)
- [Atividade geral da API do Kubernetes envolvendo o cluster do EKS](#)

Detalhes da atividade para o volume geral de chamadas de API

Os detalhes da atividade do Volume geral de chamadas de API mostram as chamadas de API que foram emitidas durante um intervalo de tempo selecionado.

Para exibir os detalhes da atividade para um único intervalo de tempo, escolha o intervalo de tempo no gráfico.

Para exibir os detalhes da atividade para o escopo de tempo atual, escolha Exibir detalhes do escopo de tempo.

Observe que o Detective começou a armazenar e exibir o nome do serviço para chamadas de API a partir de 14 de julho de 2021. Essa data é destacada no cronograma do painel de perfil. Para atividades que ocorreram antes dessa data, o nome do serviço é Serviço desconhecido.

Conteúdo dos detalhes da atividade (usuários, funções, contas, sessões de função, instâncias do EC2, buckets do S3)

Para usuários do IAM, perfis do IAM, contas, sessões de função, instâncias do EC2 e buckets do S3, os detalhes da atividade contêm as seguintes informações:

- Cada guia fornece informações sobre o conjunto de chamadas de API que foram emitidas durante o intervalo de tempo selecionado.

Para buckets do S3, as informações refletem as chamadas de API que foram feitas para o bucket do S3.

As chamadas de API são agrupadas pelos serviços que fizeram as chamadas. Para buckets do S3, o serviço é sempre o Amazon S3. Se o Detective não conseguir determinar o serviço que emitiu uma chamada, a chamada será listada em Serviço desconhecido.

- Para cada entrada, os detalhes da atividade mostram o número de chamadas bem-sucedidas e malsucedidas. A guia Endereços IP observados também mostra a localização de cada endereço IP.
- Cada entrada mostra informações sobre quem fez as chamadas. Para contas, os detalhes da atividade identificam os usuários ou as funções. Para funções, os detalhes da atividade identificam as sessões de função. Para usuários e sessões de função, os detalhes da atividade identificam os identificadores da chave de acesso (AKIDs).

Observe que, a partir de 14 de julho de 2021, para perfis de conta, os detalhes da atividade mostram usuários ou funções em vez dos AKIDs. Para perfis de função, os detalhes da atividade mostram sessões de função em vez dos AKIDs. Para atividades que ocorreram antes de 14 de julho de 2021, o chamador é listado como Recurso desconhecido.

Os detalhes da atividade contêm as seguintes guias:

Endereços IP observados

Inicialmente, exibe a lista de endereços IP usados para emitir chamadas de API.

Você pode expandir cada endereço IP para exibir a lista de chamadas de API emitidas a partir desse endereço IP. As chamadas de API são agrupadas pelos serviços que fizeram as chamadas. Para buckets do S3, o serviço é sempre o Amazon S3. Se o Detective não conseguir determinar o serviço que emitiu uma chamada, a chamada será listada em Serviço desconhecido.

Em seguida, você pode expandir cada chamada de API para exibir a lista de chamadores desse endereço IP. Dependendo do perfil, o chamador pode ser um usuário, função, sessão de função ou AKID.

Showing activity: 07/08/2021, 00:00 UTC - 07/08/2021, 04:00 UTC Edit

Observed IP addresses | **API method by service** | Resource

Filter by IP CIDR, Service name, API Method name, or Resource string

IP address	Successful calls	Failed calls	Location
[redacted]	421	311	-
s3	316	311	
config	61	0	
kms	15	0	
DescribeKey	14	0	
[redacted] Role session ([redacted])	14	0	
ListKeys	1	0	
rds	7	0	
ec2	4	0	
autoscaling	3	0	
secretsmanager	2	0	
guardduty	2	0	
es	2	0	

Método de API por serviço

Inicialmente, exibe a lista de chamadas de API que foram emitidas. As chamadas de API são agrupadas pelos serviços que fizeram as chamadas. Para buckets do S3, o serviço é sempre o Amazon S3. Se o Detective não conseguir determinar o serviço que emitiu uma chamada, a chamada será listada em Serviço desconhecido.

Você pode expandir cada método de API para exibir a lista de endereços IP dos quais as chamadas foram emitidas.

Em seguida, você pode expandir cada endereço IP para exibir a lista de AKIDs que emitiram as chamadas de API a partir desse endereço IP.

Showing activity: 07/08/2021, 00:00 UTC - 07/08/2021, 04:00 UTC Edit

Observed IP addresses | **API method by service** | Resource

Filter by IP CIDR, Service name, API Method name, or Resource string

API method	Successful calls	Failed calls
s3	316	311
config	61	0
kms	15	0
DescribeKey	14	0
[redacted]	14	0
[redacted] Role session ([redacted])	14	0
ListKeys	1	0
rds	7	0
ec2	4	0
autoscaling	3	0

Recurso ou ID da chave de acesso

Inicialmente, exibe a lista de usuários, funções, sessões de função ou AKIDs que foram usados para emitir chamadas de API.

Você pode expandir cada chamador para exibir a lista de endereços IP dos quais as chamadas de API foram emitidas.

Em seguida, você pode expandir cada endereço IP para exibir a lista de chamadas de API emitidas a partir desse endereço IP por esse chamador. As chamadas de API são agrupadas pelos serviços que fizeram as chamadas. Para buckets do S3, o serviço é sempre o Amazon S3. Se o Detective não conseguir determinar o serviço que emitiu a chamada, ela será listada em Serviço desconhecido.

The screenshot shows the 'Resource' tab in the Amazon Detective console. It displays a table of API calls grouped by resource. The table has three columns: 'Resource', 'Successful calls', and 'Failed calls'. The resources listed include 'Role session', 'kms', 'ec2', 'secretsmanager', and 'guardduty'. The 'kms' resource is expanded to show specific API methods like 'DescribeKey' and 'ListKeys'.

Resource	Successful calls	Failed calls
Role session	322	310
Role session	91	0
Role session	91	0
config	61	0
kms	15	0
DescribeKey	14	0
ListKeys	1	0
ec2	3	0
secretsmanager	2	0
guardduty	2	0
...

Conteúdo dos detalhes da atividade (endereços IP)

Para endereços IP, os detalhes da atividade contêm as seguintes informações:

- Cada guia fornece informações sobre o conjunto de chamadas de API que foram emitidas durante o intervalo de tempo selecionado. As chamadas de API são agrupadas pelos serviços que fizeram as chamadas. Se o Detective não conseguir determinar o serviço que emitiu uma chamada, a chamada será listada em Serviço desconhecido.
- Para cada entrada, os detalhes da atividade mostram o número de chamadas bem-sucedidas e malsucedidas.

Os detalhes da atividade contêm as seguintes guias:

Recurso

Inicialmente, exibe a lista de recursos que emitiram chamadas de API a partir do endereço IP.

Para cada recurso, a lista inclui o nome, o tipo e a conta da AWS do recurso.

Você pode expandir cada recurso para exibir a lista de chamadas de API emitidas pelo recurso a partir desse endereço IP. As chamadas de API são agrupadas pelos serviços que fizeram as chamadas. Se o Detective não conseguir determinar o serviço que emitiu uma chamada, a chamada será listada em Serviço desconhecido.

Showing activity: 07/08/2021, 00:00 UTC - 07/08/2021, 04:00 UTC Edit

Resource | API method by service

Filter by Resource string, Service name or API Method name

Resource	Successful calls	Failed calls	Account ID
<ul style="list-style-type: none"> config <ul style="list-style-type: none"> DescribeComplianceByConfigRule PutEvaluations SelectResourceConfig DescribeDeliveryChannelStatus DescribeConfigurationRecorderSta... DescribeConfigurationRecorders ec2 shield waf-regional 	3,520	0	
	1,754	0	
	1,408	0	
	244	0	
	78	0	
	8	0	
	8	0	
	8	0	
	1,690	0	
	50	0	
	26	0	
	1,715	0	
	504	480	

Método de API por serviço

Inicialmente, exibe a lista de chamadas de API que foram emitidas. As chamadas de API são agrupadas pelos serviços que fizeram as chamadas. Se o Detective não conseguir determinar o serviço que emitiu uma chamada, a chamada será listada em Serviço desconhecido.

Você pode expandir cada chamada de API para exibir a lista de recursos que emitiram a chamada de API a partir do endereço IP durante o período selecionado.

Showing activity: 07/08/2021, 00:00 UTC - 07/08/2021, 04:00 UTC Edit

Resource | API method by service

Filter by Resource string, Service name or API Method name

API method	Successful calls	Failed calls
config	3,787	0
ec2	2,538	0
s3	1,269	1,016
<ul style="list-style-type: none"> ssm <ul style="list-style-type: none"> ListCommands <ul style="list-style-type: none"> AWS role () AWS role () SendCommand 	481	16
	392	0
	222	0
	170	0
	89	16
logs	165	0
sts	149	0
iam	149	12

Classificar os detalhes da atividade

Você pode classificar os detalhes da atividade por qualquer uma das colunas da lista.

Ao classificar usando a primeira coluna, somente a lista de nível superior é classificada. As listas de nível inferior são sempre classificadas pela contagem de chamadas de API bem-sucedidas.

Filtrar os detalhes da atividade

Você pode usar as opções de filtragem para se concentrar em subconjuntos ou aspectos específicos da atividade representados nos detalhes da atividade.

Em todas as guias, você pode filtrar a lista por qualquer um dos valores na primeira coluna.

Para adicionar um filtro

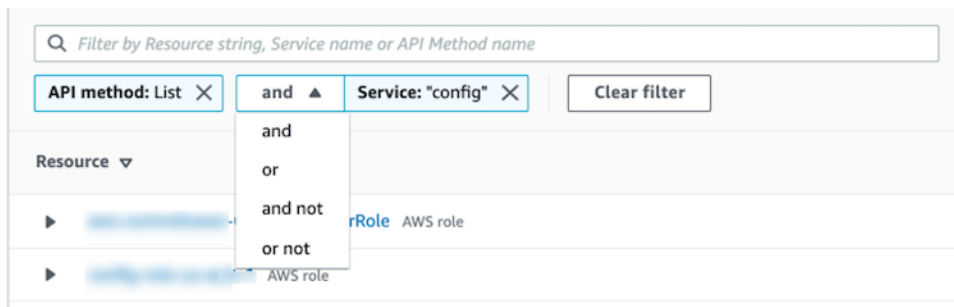
1. Escolha a caixa de filtro.
2. Em Propriedades, escolha a propriedade a ser usada para a filtragem.
3. Forneça o valor a ser usado para a filtragem. O filtro comporta valores parciais. Por exemplo, ao filtrar por método de API, se você filtrar por **Instance**, os resultados incluem qualquer operação de API que tenha Instance em seu nome. Então, ambos `ListInstanceAssociations` e `UpdateInstanceInformation` corresponderiam.

Para nomes de serviços, métodos de API e endereços IP, você pode especificar um valor ou escolher um filtro incorporado.

Para Substrings comuns de API, escolha a substring que representa o tipo de operação, tal como `List`, `Create` ou `Delete`. Cada nome de método de API começa com o tipo de operação.

Para Padrões CIDR, você pode optar por incluir somente endereços IP públicos, endereços IP privados ou endereços IP que correspondam a um padrão CIDR específico.

4. Se você tiver vários filtros, escolha uma opção booliana para definir como esses filtros são conectados.



5. Para remover um filtro, escolha o ícone x no canto superior direito.

6. Para limpar todos os filtros, escolha Limpar filtro.

Selecionar o intervalo de tempo dos detalhes da atividade

Ao exibir pela primeira vez os detalhes da atividade, o intervalo de tempo é o escopo de tempo ou um intervalo de tempo selecionado. Você pode alterar o intervalo de tempo dos detalhes da atividade.

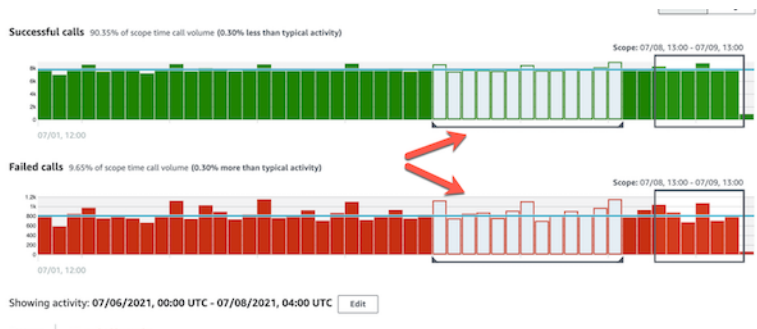
Para alterar o intervalo de tempo dos detalhes da atividade

1. Selecione a opção Editar.
2. Em Editar janela de tempo, escolha o horário de início e de término a ser usado.

Para definir a janela de tempo como o escopo de tempo padrão do perfil, escolha Definir como o escopo de tempo padrão.

3. Escolha a Atualizar janela de tempo.

O intervalo de tempo dos detalhes da atividade é destacado nos gráficos do painel de perfil.



Consultar logs brutos

O Amazon Detective se integra ao Amazon Security Lake, o que significa que você pode consultar e recuperar os dados de log bruto armazenados pelo Security Lake. Para obter mais detalhes sobre essa interação, consulte [Integração com o Amazon Security Lake](#).

Usando essa integração, você pode coletar logs e eventos das fontes a seguir, às quais o Security Lake oferece suporte nativo.

- AWS CloudTrail eventos de gerenciamento
- Logs de fluxo do Amazon Virtual Private Cloud (Amazon VPC)

Note

Não há cobranças adicionais pela consulta de logs de dados brutos no Detective. As taxas de uso de outros AWS Serviços, incluindo o Amazon Athena, ainda se aplicam às tarifas publicadas.

Como consultar logs brutos

1. Selecione exibir detalhes do tempo do escopo.
2. Neste ponto, você pode começar a Consultar logs brutos.
3. Na tabela de Visualização do log bruto, é possível visualizar os logs e eventos recuperados consultando dados do Security Lake. Para obter mais detalhes sobre os logs de eventos brutos, você pode visualizar os dados exibidos no Amazon Athena.

Na tabela Consultar logs brutos, você pode Cancelar solicitação de consulta, Ver resultados no Amazon Athena e Baixar resultados como um arquivo de valores separados por vírgula (.csv).

Se você ver logs no Detective, mas a consulta não retornou nenhum resultado, existem alguns motivos pelos quais isso pode ter acontecido.

- Os logs brutos podem ficar disponíveis no Detective antes de aparecerem nas tabelas de log do Security Lake. Tente novamente mais tarde.
- Os logs podem estar ausentes do Security Lake. Se você esperou por um longo período, isso indica que faltam logs do Security Lake. Entre em contato com o administrador do Security Lake para resolver o problema.

Detalhes da atividade para uma geolocalização

Os detalhes da atividade de Geolocalizações recém-observadas mostram as chamadas de API emitidas de uma geolocalização durante o escopo de tempo. As chamadas de API incluem todas as chamadas emitidas a partir da geolocalização. Não estão limitadas às chamadas que usaram a entidade da descoberta ou do perfil. Para buckets do S3, as chamadas da atividade são chamadas de API feitas para o bucket do S3.

Detective determina a localização das solicitações usando bancos de dados GeoIP MaxMind . MaxMind relata uma precisão muito alta de seus dados em nível de país, embora a precisão varie de

acordo com fatores como país e tipo de IP. Para obter mais informações sobre MaxMind, consulte [Geolocalização MaxMind IP](#). [Se achar que algum dado do GeoIP está incorreto, você pode enviar uma solicitação de correção para a Maxmind em MaxMind Correct GeoIP2 Data](#).

As chamadas de API são agrupadas pelos serviços que fizeram as chamadas. Para buckets do S3, o serviço é sempre o Amazon S3. Se o Detective não conseguir determinar o serviço que emitiu uma chamada, a chamada será listada em Serviço desconhecido.

Para exibir os detalhes da atividade, realize uma destas ações:

- No mapa, escolha uma geolocalização.
- Na lista, escolha Detalhes de uma geolocalização.

Os detalhes da atividade substituem a lista de geolocalizações. Para retornar à lista de geolocalizações, escolha Retornar para todos os resultados.

Observe que o Detective começou a armazenar e exibir o nome do serviço para chamadas de API a partir de 14 de julho de 2021. Para atividades que ocorreram antes dessa data, o nome do serviço é Serviço desconhecido.

Conteúdo dos detalhes da atividade

Cada guia fornece informações sobre todas as chamadas de API emitidas a partir da geolocalização durante o escopo de tempo.

Para cada endereço IP, recurso e método de API, a lista mostra o número de chamadas de API bem-sucedidas e malsucedidas.

Os detalhes da atividade contêm as seguintes guias:

Endereços IP observados

Inicialmente, exibe a lista de endereços IP que foram usados para emitir chamadas de API a partir da geolocalização selecionada.

Você pode expandir cada endereço IP para exibir os recursos que emitiram chamadas de API a partir desse endereço IP. A lista exibe o nome do recurso. Para ver o ID da entidade principal, passe o mouse sobre o nome.

Em seguida, você pode expandir cada recurso para exibir as chamadas de API específicas emitidas a partir desse endereço IP por esse recurso. As chamadas de API são agrupadas pelos

serviços que fizeram as chamadas. Para buckets do S3, o serviço é sempre o Amazon S3. Se o Detective não conseguir determinar o serviço que emitiu uma chamada, a chamada será listada em Serviço desconhecido.

Ashburn, US from 05/14/2021 - 06/28/2021

Observed IP addresses | Resource

Filter by IP CIDR, API Method name, or Resource string

IP address	Successful calls	Failed calls
[Redacted]	27,564	2,453
[Redacted] AWS role ([Redacted])	27,564	2,453
ssm	25,111	0
UpdateInstanceInformation	13,066	0
ListInstanceAssociations	6,482	0
PutInventory	2,544	0
GetDeployablePatchSnapshotForIns...	2,453	0
UpdateInstanceAssociationStatus	466	0
PutComplianceItems	98	0
GetDocument	2	0
sts	2,453	0
s3	0	2,453
[Redacted]	24,635	1,512
[Redacted]	24,632	1,511

Recurso

Inicialmente, exibe a lista de recursos que emitiram chamadas de API a partir da geolocalização selecionada. A lista exibe o nome do recurso. Para ver a ID da entidade principal, pause no nome. Para cada recurso, a guia Recurso também exibe a Conta da AWS associada.

Você pode expandir cada usuário ou função para exibir a lista de chamadas de API emitidas por esse recurso. As chamadas de API são agrupadas pelos serviços que fizeram as chamadas. Para buckets do S3, o serviço é sempre o Amazon S3. Se o Detective não conseguir determinar o serviço que emitiu uma chamada, a chamada será listada em Serviço desconhecido.

Em seguida, você pode expandir cada chamada de API para exibir a lista de endereços IP dos quais o recurso emitiu a chamada de API.

Ashburn, US from 05/14/2021 - 06/28/2021

Observed IP addresses | Resource

Filter by IP CIDR, API Method name, or Resource string

Resource	Successful calls	Failed calls	Account ID
[Redacted] AWS role	189,097	17	[Redacted]
[Redacted] AWS role	49,267	3,023	[Redacted]
ssm	46,254	0	
UpdateInstanceInformation	25,932	0	
[Redacted]	12,968	0	
[Redacted]	12,964	0	
ListInstanceAssociations	12,964	0	
PutInventory	3,194	0	
GetDeployablePatchSnapshotForIns...	3,011	0	
UpdateInstanceAssociationStatus	949	0	
PutComplianceItems	199	0	
GetDocument	5	0	
sts	3,013	0	
s3	0	3,023	

Classificar os detalhes da atividade

Você pode classificar os detalhes da atividade por qualquer uma das colunas da lista.

Ao classificar usando a primeira coluna, somente a lista de nível superior é classificada. As listas de nível inferior são sempre classificadas pela contagem de chamadas de API bem-sucedidas.

Filtrar os detalhes da atividade

Você pode usar as opções de filtragem para se concentrar em subconjuntos ou aspectos específicos da atividade representados nos detalhes da atividade.

Em todas as guias, você pode filtrar a lista por qualquer um dos valores na primeira coluna.

Para adicionar um filtro

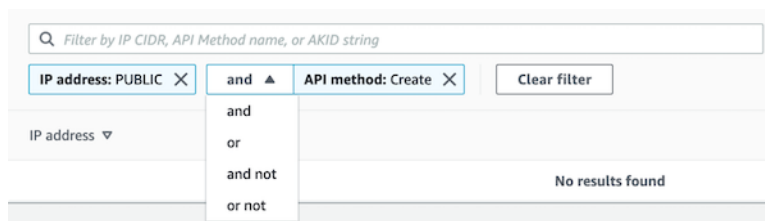
1. Escolha a caixa de filtro.
2. Em Propriedades, escolha a propriedade a ser usada para a filtragem.
3. Forneça o valor a ser usado para a filtragem. O filtro comporta valores parciais. Por exemplo, ao filtrar por método de API, se você filtrar por **Instance**, os resultados incluem qualquer operação de API que tenha Instance em seu nome. Então, ambos `ListInstanceAssociations` e `UpdateInstanceInformation` corresponderiam.

Para nomes de serviços, métodos de API e endereços IP, você pode especificar um valor ou escolher um filtro incorporado.

Para Substrings comuns de API, escolha a substring que representa o tipo de operação, tal como `List`, `Create` ou `Delete`. Cada nome de método de API começa com o tipo de operação.

Para Padrões CIDR, você pode optar por incluir somente endereços IP públicos, endereços IP privados ou endereços IP que correspondam a um padrão CIDR específico.

4. Se você tiver vários filtros, escolha uma opção booleana para definir como esses filtros são conectados.



5. Para remover um filtro, escolha o ícone x no canto superior direito.
6. Para limpar todos os filtros, escolha Limpar filtro.

Detalhes da atividade para o volume geral de fluxo do VPC

Para uma instância do EC2, os detalhes da atividade em Volume geral de fluxo do VPC mostram as interações entre a instância do EC2 e os endereços IP durante um intervalo de tempo selecionado.

Para um pod do Kubernetes, Volume geral de fluxo do VPC exibe o volume geral de bytes que entram e saem do endereço IP atribuído ao pod do Kubernetes para todos os endereços IP de destino. O endereço IP do pod do Kubernetes não é exclusivo quando `hostNetwork: true`. Nesse caso, o painel mostra o tráfego para outros pods com a mesma configuração e o nó que os hospeda.

Para um endereço IP, os detalhes da atividade em Volume geral de fluxo do VPC mostram as interações entre o endereço IP e as instâncias do EC2 durante um intervalo de tempo selecionado.

Para exibir os detalhes da atividade para um único intervalo de tempo, escolha o intervalo de tempo no gráfico.

Para exibir os detalhes da atividade do escopo de tempo atual, escolha Exibir detalhes do escopo de tempo.

Conteúdo dos detalhes da atividade

O conteúdo reflete a atividade durante o intervalo de tempo selecionado.

Para uma instância do EC2, os detalhes da atividade contêm uma entrada para cada combinação exclusiva de endereço IP, porta local, porta remota, protocolo e direção.

Para um endereço IP, os detalhes da atividade contêm uma entrada para cada combinação exclusiva de instância do EC2, porta local, porta remota, protocolo e direção.

Cada entrada exibe o volume do tráfego de entrada, o volume do tráfego de saída e se a solicitação de acesso foi aceita ou rejeitada. Nos perfis de descobertas, a coluna Anotações indica quando um endereço IP está relacionado à descoberta atual.

IP address	Local port	Remote port	Inbound traffic	Outbound traffic	Protocol	Directionality	Accept / Reject	Annotations
10.0.0.1	-	4444	596 B	9.43 kB	TCP	Outbound	Accept	From Finding
10.0.0.1	-	4444	596 B	23.3 kB	TCP	Outbound	Accept	From Finding
10.0.0.1	-	4444	268 B	9.09 kB	TCP	Outbound	Accept	From Finding
10.0.0.1	-	4444	216 B	5.93 kB	TCP	Outbound	Accept	From Finding
10.0.0.1	-	4444	216 B	6.07 kB	TCP	Outbound	Accept	From Finding
10.0.0.1	-	4444	164 B	10.8 kB	TCP	Outbound	Accept	From Finding
10.0.0.1	-	4444	164 B	8.77 kB	TCP	Outbound	Accept	From Finding
10.0.0.1	22	2264	7.75 MB	13.3 MB	TCP	Unknown	Accept	
10.0.0.1	-	53	2.59 MB	2.08 MB	UDP	Unknown	Accept	

Classificar os detalhes da atividade

Você pode classificar os detalhes da atividade por qualquer uma das colunas na tabela.

Por padrão, os detalhes da atividade são classificados primeiro pelas anotações e depois pelo tráfego de entrada.

Filtrar os detalhes da atividade

Para se concentrar em uma atividade específica, você pode filtrar os detalhes da atividade pelos seguintes valores:

- Endereço IP ou instância do EC2
- Porta local ou remota
- Direction
- Protocolo
- Se a solicitação foi aceita ou rejeitada

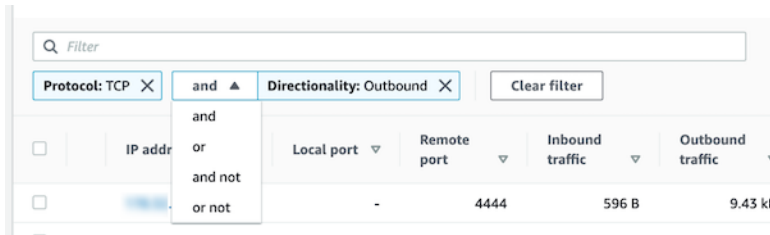
Para adicionar e remover filtros

1. Escolha a caixa de filtro.
2. Em Propriedades, escolha a propriedade a ser usada para a filtragem.
3. Forneça o valor a ser usado para a filtragem. O filtro comporta valores parciais.

Para filtrar por endereço IP, você pode especificar um valor ou escolher um filtro incorporado.

Para Padrões CIDR, você pode optar por incluir somente endereços IP públicos, endereços IP privados ou endereços IP que correspondam a um padrão CIDR específico.

- Se você tiver vários filtros, escolha uma opção booliana para definir como esses filtros são conectados.



- Para remover um filtro, escolha o ícone x no canto superior direito.
- Para limpar todos os filtros, escolha Limpar filtro.

Selecionar o intervalo de tempo dos detalhes da atividade

Ao exibir pela primeira vez os detalhes da atividade, o intervalo de tempo é o escopo de tempo ou um intervalo de tempo selecionado. Você pode alterar o intervalo de tempo dos detalhes da atividade.

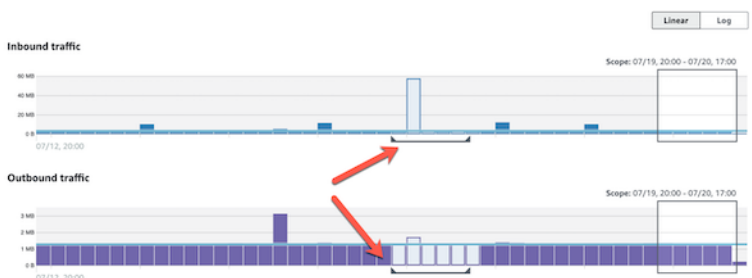
Para alterar o intervalo de tempo dos detalhes da atividade

- Selecione a opção Editar.
- Em Editar janela de tempo, escolha o horário de início e de término a ser usado.

Para definir a janela de tempo como o escopo de tempo padrão do perfil, escolha Definir como o escopo de tempo padrão.

- Escolha a Atualizar janela de tempo.

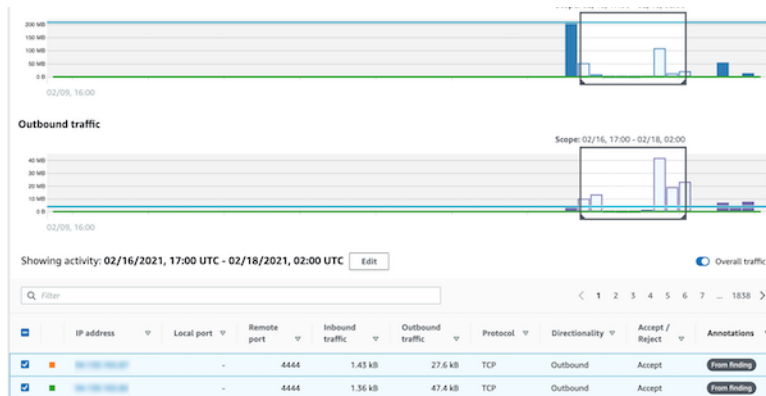
O intervalo de tempo dos detalhes da atividade é destacado nos gráficos do painel de perfil.



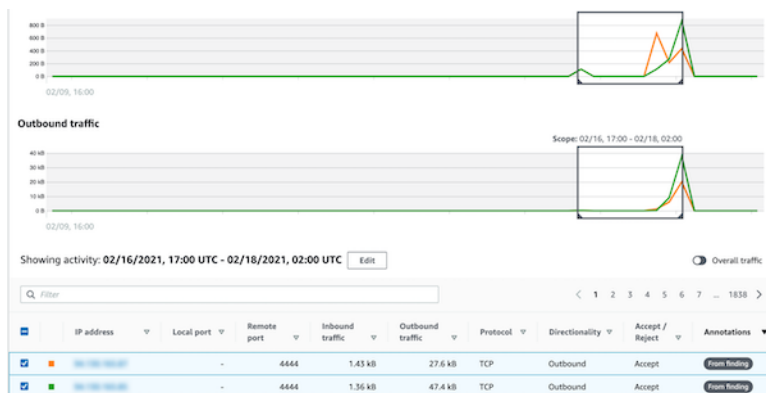
Exibir o volume de tráfego das linhas selecionadas

Ao identificar as linhas de interesse, você pode exibir nos gráficos principais o volume de tráfego dessas linhas ao longo do tempo.

Para cada linha a ser adicionada aos gráficos, marque a caixa de seleção. Para cada linha selecionada, o volume é exibido como uma linha nos gráficos de entrada ou saída.



Para se concentrar no volume de tráfego das entradas selecionadas, você pode ocultar o volume geral. Para mostrar ou ocultar o volume geral de tráfego, ative Tráfego geral.



Exibir o tráfego de fluxo do VPC para clusters do EKS

O Detective tem visibilidade dos seus logs de fluxo do Amazon Virtual Private Cloud (Amazon VPC), que representam o tráfego que atravessa seus clusters do Amazon Elastic Kubernetes Service (Amazon EKS). Para recursos do Kubernetes, o conteúdo dos logs de fluxo do VPC depende do CNI (Container Network Interface) implantado no cluster do EKS.

Um cluster do EKS com uma configuração padrão usa o plugin Amazon VPC CNI. Para obter mais detalhes, consulte [Gerenciar o VPC CNI](#) no Guia do usuário do Amazon EKS. O plugin Amazon VPC CNI envia tráfego interno com o endereço IP do pod e traduz o endereço IP de origem para o endereço IP do nó para comunicação externa. O Detective pode capturar e correlacionar o tráfego interno ao pod correto, mas não pode fazer o mesmo com o tráfego externo.

Se você quiser que o Detective tenha visibilidade do tráfego externo de seus pods, habilite a Tradução de endereços de rede de fonte externa (SNAT). A habilitação da SNAT traz limitações e

desvantagens. Para obter mais detalhes, consulte [SNAT para pods](#) no Guia do usuário do Amazon EKS.

Se você usa um plugin do CNI diferente, o Detective tem visibilidade limitada aos pods com `hostNetwork:true`. Para esses pods, o painel Fluxo do VPC exibe todo o tráfego para o endereço IP do pod. Isso inclui o tráfego para o nó do host e qualquer pod no nó com a configuração `hostNetwork:true`.

O Detective exibe o tráfego no painel Fluxo do VPC de um pod do KS para as seguintes configurações de cluster do EKS:

- Em um cluster com o plugin Amazon VPC CNI, qualquer pod com a configuração `hostNetwork:false` que envia tráfego dentro do VPC do cluster.
- Em um cluster com o plugin Amazon VPC CNI e a configuração `AWS_VPC_K8S_CNI_EXTERNALSNAT=true`, qualquer pod com `hostNetwork:false` que envia tráfego fora do VPC do cluster.
- Qualquer pod com a configuração `hostNetwork:true`. O tráfego do nó é misturado com o tráfego de outros pods que têm a configuração `hostNetwork:true`.

O Detective não exibe o tráfego no painel Fluxo do VPC para:

- Em um cluster com o plugin Amazon VPC CNI e a configuração `AWS_VPC_K8S_CNI_EXTERNALSNAT=false`, qualquer pod com a configuração `hostNetwork:false` que envia tráfego fora do VPC do cluster.
- Em um cluster sem o plugin Amazon VPC CNI para o Kubernetes, qualquer pod com a configuração `hostNetwork:false`.
- Qualquer pod que envia tráfego para outro pod hospedado no mesmo nó.

Exibir o tráfego de fluxo da VPC para Amazon VPCs compartilhados

O Detective tem visibilidade sobre os logs de fluxo da Amazon Virtual Private Cloud (Amazon VPC) para VPCs compartilhados:

- Se uma conta-membro do Detective tiver um Amazon VPC compartilhado e houver outras contas que não são do Detective usando a VPC compartilhada, o Detective monitora todo o tráfego dessa VPC e fornece visualização sobre todo o fluxo de tráfego dentro da VPC.

- Se você tiver uma instância do Amazon EC2 dentro de um Amazon VPC compartilhado e o proprietário compartilhado da VPC não for membro do Detective, o Detective não monitorará nenhum tráfego da VPC. Se você quiser visualizar o fluxo de tráfego dentro da VPC, deverá adicionar o proprietário do Amazon VPC como membro do seu gráfico do Detective.

Atividade geral da API do Kubernetes envolvendo o cluster do EKS

Os detalhes da atividade em Atividade geral da API do Kubernetes envolvendo o cluster do EKS mostram o número de chamadas de API do Kubernetes bem-sucedidas e malsucedidas emitidas durante um intervalo de tempo selecionado.

Para exibir os detalhes da atividade para um único intervalo de tempo, escolha o intervalo de tempo no gráfico.

Para exibir os detalhes da atividade para o escopo de tempo atual, escolha Exibir detalhes do escopo de tempo.

Conteúdo dos detalhes da atividade (cluster, pod, usuário, função, sessão de função)

Para um cluster, pod, usuário, função ou sessão de função, os detalhes da atividade contêm as seguintes informações:

- Cada guia fornece informações sobre o conjunto de chamadas de API que foram emitidas durante o intervalo de tempo selecionado.

Para clusters, as chamadas de API ocorreram dentro do cluster.

Para pods, as chamadas de API foram direcionadas ao pod.

Para usuários, funções e sessões de função, as chamadas de API foram emitidas por usuários do Kubernetes que se autenticaram como esse usuário, função ou sessão de função.

- Para cada entrada, os detalhes da atividade mostram o número de chamadas bem-sucedidas, malsucedidas, não autorizadas e proibidas.
- As informações incluem o endereço IP, o tipo de chamada do Kubernetes, a entidade afetada pela chamada e o sujeito (conta de serviço ou usuário) que fez a chamada. A partir dos detalhes da atividade, você pode acessar os perfis do endereço IP, do sujeito e da entidade afetada.

Os detalhes da atividade contêm as seguintes guias:

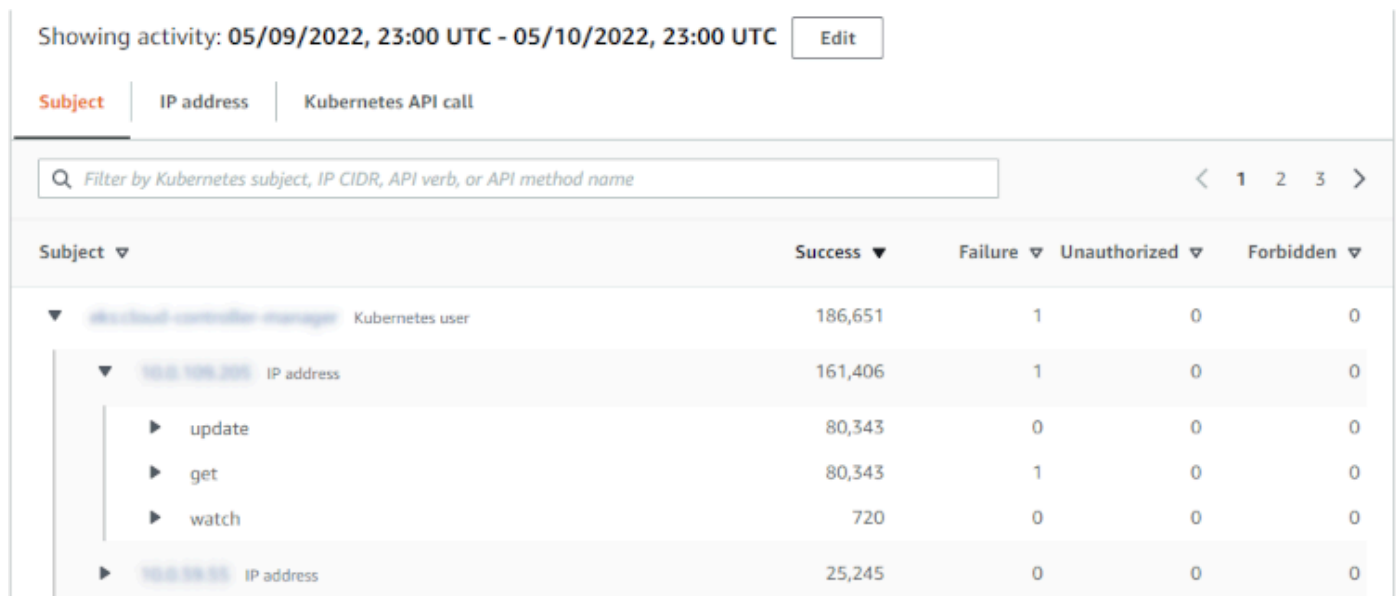
Sujeito

Inicialmente, exibe a lista de contas de serviço e usuários que foram usados para fazer chamadas de API.

Você pode expandir cada conta de serviço e usuário para exibir a lista de endereços IP a partir dos quais a conta ou o usuário fez chamadas de API.

Em seguida, você pode expandir cada endereço IP para mostrar as chamadas de API do Kubernetes que foram feitas por essa conta ou usuário a partir desse endereço IP.

Expanda a chamada de API do Kubernetes para ver a `requestURI` e identificar a ação realizada.



The screenshot shows a table of API call activity. At the top, it indicates the time range: "Showing activity: 05/09/2022, 23:00 UTC - 05/10/2022, 23:00 UTC" with an "Edit" button. Below this are three tabs: "Subject", "IP address", and "Kubernetes API call". The "Subject" tab is selected. A search bar is present with the placeholder text "Filter by Kubernetes subject, IP CIDR, API verb, or API method name". The table has five columns: "Subject", "Success", "Failure", "Unauthorized", and "Forbidden". The data is as follows:

Subject	Success	Failure	Unauthorized	Forbidden
awscloud-controller-manager Kubernetes user	186,651	1	0	0
10.0.100.200 IP address	161,406	1	0	0
▶ update	80,343	0	0	0
▶ get	80,343	1	0	0
▶ watch	720	0	0	0
▶ 10.0.100.50 IP address	25,245	0	0	0

Endereço IP

Inicialmente, exibe a lista de endereços IP a partir dos quais as chamadas de API foram emitidas.

Você pode expandir cada chamada para exibir a lista de sujeitos do Kubernetes (contas de serviço e usuários) que fizeram a chamada.

Em seguida, você pode expandir cada sujeito para exibir a lista de tipos de chamadas de API feitas pelo sujeito durante o escopo de tempo.

Expanda o tipo de chamada de API para ver a `requestURI` e identificar a ação realizada.

Showing activity: 05/09/2022, 23:00 UTC - 05/10/2022, 23:00 UTC Edit

Subject | **IP address** | Kubernetes API call

Filter by Kubernetes subject, IP CIDR, API verb, or API method name

IP address	Success	Failure	Unauthorized	Forbidden	Location
10.0.1.1 IP address	599,250	2,706	0	0	-
awscloud-controller-manager Kubernetes user	161,406	1	0	0	
update	80,343	0	0	0	
/apis/coordination.k8s.io/v1/namespaces/kube-system/leases/cloud-provider-extraction-migration	40,172	0	0	0	
/apis/coordination.k8s.io/v1/namespaces/kube-system/leases/cloud-controller-manager	40,171	0	0	0	

Chamada de API do Kubernetes

Inicialmente, exibe a lista de verbos de chamadas de API do Kubernetes.

Você pode expandir cada verbo da API para exibir as requestURIs associadas a essa ação.

Em seguida, você pode expandir cada requestURI para ver os sujeitos do Kubernetes (contas de serviço e usuários) que fizeram a chamada.

Expanda o sujeito para ver quais IPs esse sujeito usou para fazer a chamada de API.

Showing activity: 07/08/2021, 00:00 UTC - 07/08/2021, 04:00 UTC Edit

Observed IP addresses | API method by service | **Resource**

Filter by IP CIDR, Service name, API Method name, or Resource string

Resource	Successful calls	Failed calls
Role session	322	310
Role session	91	0
config	91	0
kms	61	0
DescribeKey	15	0
ListKeys	14	0
ec2	1	0
secretsmanager	3	0
guardduty	2	0
...	2	0

Classificar os detalhes da atividade

Você pode classificar os detalhes da atividade por qualquer uma das colunas da lista.

Ao classificar usando a primeira coluna, somente a lista de nível superior é classificada. As listas de nível inferior são sempre classificadas pela contagem de chamadas de API bem-sucedidas.

Filtrar os detalhes da atividade

Você pode usar as opções de filtragem para se concentrar em subconjuntos ou aspectos específicos da atividade representados nos detalhes da atividade.

Em todas as guias, você pode filtrar a lista por qualquer um dos valores na primeira coluna.

Selecionar o intervalo de tempo dos detalhes da atividade

Ao exibir pela primeira vez os detalhes da atividade, o intervalo de tempo é o escopo de tempo ou um intervalo de tempo selecionado. Você pode alterar o intervalo de tempo dos detalhes da atividade.

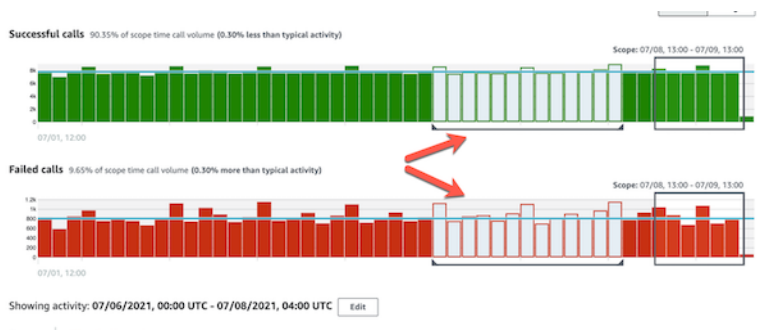
Para alterar o intervalo de tempo dos detalhes da atividade

1. Selecione a opção Editar.
2. Em Editar janela de tempo, escolha o horário de início e de término a ser usado.

Para definir a janela de tempo como o escopo de tempo padrão do perfil, escolha Definir como o escopo de tempo padrão.

3. Escolha a Atualizar janela de tempo.

O intervalo de tempo dos detalhes da atividade é destacado nos gráficos do painel de perfil.



Usar a orientação do painel de perfil durante uma investigação

Cada painel de perfil é projetado para fornecer respostas a perguntas específicas que surgem à medida que você conduz uma investigação e analisa a atividade das entidades relacionadas.

A orientação fornecida para cada painel de perfil ajuda você a encontrar essas respostas.

A orientação do painel de perfil começa com uma única frase no próprio painel. Essa orientação fornece uma breve explicação dos dados apresentados no painel.

Para exibir orientações mais detalhadas em um painel, escolha Mais informações no cabeçalho do painel. Essa orientação estendida aparece no painel de ajuda.

A orientação pode fornecer estes tipos de informações:

- Uma visão geral do conteúdo do painel
- Como usar o painel para responder às perguntas relevantes
- Próximas etapas sugeridas com base nas respostas

Navegar diretamente até o perfil de uma entidade ou até a visão geral de uma descoberta

Para navegar diretamente até o perfil de uma entidade ou até a visão geral de uma descoberta no Amazon Detective, você pode usar uma das seguintes opções.

- Da Amazon GuardDuty ou AWS Security Hub, você pode passar de uma GuardDuty descoberta para o perfil de descoberta correspondente do Detective.
- Você pode montar um URL do Detective que identifique uma descoberta ou entidade e defina o escopo de tempo a ser usado.

Navegando para um perfil de entidade ou encontrando uma visão geral da Amazon GuardDuty ou AWS Security Hub

No GuardDuty console da Amazon, você pode navegar até o perfil da entidade relacionada a uma descoberta.

Nos AWS Security Hub consoles GuardDuty e, você também pode navegar até uma visão geral das descobertas. Isso também fornece links para os perfis das entidades envolvidas.

Esses links podem ajudar a agilizar o processo de investigação. Você pode usar rapidamente o Detective para ver a atividade da entidade associada e determinar as próximas etapas. Você também pode arquivar uma descoberta se for um falso positivo ou explorar mais para determinar o escopo do problema.

Como migrar para o console do Amazon Detective

Os links da investigação estão disponíveis para todas as GuardDuty descobertas. GuardDuty também permite que você escolha se deseja navegar até um perfil de entidade ou até a visão geral da descoberta.

Para passar para Detective a partir do console GuardDuty

1. Abra o GuardDuty console em <https://console.aws.amazon.com/guardduty/>.
2. Se necessário, escolha Descobertas no painel de navegação esquerdo.
3. Na página GuardDuty Descobertas, escolha a descoberta.

O painel de detalhes da descoberta é exibido à direita da lista de descobertas.

4. Escolha Investigar no Detective no painel de detalhes da descoberta.

GuardDuty exibe uma lista de itens disponíveis para investigar em Detective.

A lista contém as entidades relacionadas, tais como endereços IP ou instâncias do EC2, e a descoberta.

5. Escolha uma entidade ou a descoberta.

O console do Detective é aberto em uma nova guia. O console é aberto no perfil da entidade ou da descoberta.

Se você não habilitou o Detective, o console abrirá em uma página inicial que fornece uma visão geral do Detective. A partir daí, você pode optar por habilitar o Detective.

Para migrar para o Detective a partir do console do Security Hub

1. Abra o AWS Security Hub console em <https://console.aws.amazon.com/securityhub/>.
2. Se necessário, escolha Descobertas no painel de navegação esquerdo.
3. Na página Descobertas do Security Hub, escolha uma GuardDuty descoberta.
4. No painel de detalhes, escolha Investigar no Detective e, em seguida, escolha Investigar descoberta.

Quando você escolhe Investigar descoberta, o console do Detective é aberto em uma nova guia. O console abre na visão geral da descoberta.

O console do Detective sempre abre na região de origem da descoberta, mesmo que você saia da região de agregação. Para obter mais informações sobre agregação de descobertas, consulte [Agregar descobertas entre regiões](#) no Guia do usuário do AWS Security Hub .

Se você não habilitou o Detective, o console abrirá na página inicial do Detective. A partir daí, você pode habilitar o Detective.

Solução de problemas de migração

Para usar a migração, uma das opções a seguir deve ser verdadeira:

- Sua conta deve ser uma conta de administrador do Detective e do serviço do qual você estiver migrando.
- Você assumiu uma função entre contas que concede à sua conta de administrador acesso ao gráfico de comportamento.

Para obter mais informações sobre a recomendação de alinhar contas de administrador, consulte [Alinhamento recomendado com a Amazon e. GuardDuty AWS Security Hub](#)

Se a migração não funcionar, verifique o seguinte.

- A descoberta pertence a uma conta-membro habilitada em seu gráfico de comportamento? Se a conta associada não tiver sido convidada para o gráfico de comportamento como uma conta-membro, o gráfico de comportamento não conterá dados dessa conta.

Se uma conta-membro convidada não tiver aceitado o convite, o gráfico de comportamento não conterá dados dessa conta.

- A descoberta está arquivada? Detective não recebe descobertas arquivadas de. GuardDuty
- A descoberta ocorreu antes de o Detective iniciar a ingestão de dados em seu gráfico de comportamento? Se a descoberta não estiver presente nos dados que o Detective ingeriu, o gráfico de comportamento não conterá os dados dela.
- A descoberta é da região correta? Cada gráfico de comportamento é específico de uma região. Um gráfico de comportamento não contém dados de outras regiões.

Navegar até o perfil de uma entidade ou até a visão geral de uma descoberta usando um URL

Para navegar até o perfil de uma entidade ou até a visão geral de uma descoberta no Amazon Detective, você pode usar um URL que fornece um link direto a eles. O URL identifica a descoberta ou a entidade. Ele também pode especificar o escopo de tempo a ser usado no perfil. O Detective mantém até um ano do histórico de dados de eventos.

Formato do URL de um perfil

Note

Se você estiver usando o formato de URL antigo, o Detective redirecionará automaticamente para o novo URL. O formato de URL antigo era:

```
https://console.aws.amazon.com/detective/home?  
region=Region#type/namespace/instanceID?parameters
```

O novo formato do URL do perfil é o seguinte:

- Para entidades: `https://console.aws.amazon.com/detective/home?region=Region#entities/namespace/instanceID?parameters`
- Para descobertas: `https://console.aws.amazon.com/detective/home?region=Region#findings/instanceID?parameters`

O URL exige os seguintes valores.

Region

A região que você deseja usar.

tipo

O tipo de item do perfil para o qual você está navegando.

- `entities`: indica que você está navegando até o perfil de uma entidade
- `findings`: indica que você está navegando para a visão geral de uma descoberta

namespace

Para entidades, o namespace é o nome do tipo de entidade.

- `AwsAccount`
- `AwsRole`
- `AwsRoleSession`
- `AwsUser`
- `Ec2Instance`
- `FederatedUser`
- `IpAddress`
- `S3Bucket`
- `UserAgent`
- `FindingGroup`
- `KubernetesSubject`
- `ContainerPod`
- `ContainerCluster`
- `ContainerImage`

instanceID

O identificador da instância da descoberta ou da entidade.

- Para uma GuardDuty descoberta, o identificador da GuardDuty descoberta.
- Para uma AWS conta, o ID da conta.
- Para AWS funções e usuários, a ID principal da função ou do usuário.
- Para usuários federados, a ID principal do usuário federado.
A ID principal é `<identityProvider>:<username>` ou `<identityProvider>:<audience>:<username>`.
- Para endereços IP, o endereço IP.
- Para agentes de usuário, o nome do agente de usuário.
- Para instâncias do EC2, a ID da instância.
- Para sessões de função, o identificador da sessão. O identificador da sessão usa o formato `<rolePrincipalID>:<sessionName>`.
- Para buckets do S3, o nome do bucket.
- Para FindingGroups, um UUID. por exemplo, ca6104bc-a315-4b15-bf88-1c1e60998f83
- Para recursos do EKS, use os seguintes formatos:
 - Cluster do EKS: `<clusterName>~<accountId>~EKS`

- Pod do Kubernetes: `<podUid>~<clusterName><accountId>~EKS`
- Sujeito do Kubernetes: `<subjectName>~<clusterName>~<accountId>`
- Imagem de contêiner: `<registry>/<repository>:<tag>@<digest>`

A descoberta ou entidade deve estar associada a uma conta habilitada em seu gráfico de comportamento.

O URL também pode incluir os seguintes parâmetros opcionais, que são usados para definir o escopo de tempo. Para obter mais informações sobre o escopo de tempo e como ele é usado nos perfis, consulte [the section called “Gerenciar o escopo de tempo”](#).

scopeStart

Hora de início do escopo de tempo a ser usado no perfil. A hora de início deve estar nos últimos 365 dias.

O valor é o epoch timestamp.

Se você fornecer uma hora de início, mas não uma hora de término, o escopo de tempo terminará na hora atual.

scopeEnd

Hora de término do escopo de tempo a ser usado no perfil.

O valor é o epoch timestamp.

Se você fornecer uma hora de término, mas não uma hora de início, o escopo de tempo incluirá todo o tempo antes da hora de término.

Se você não especificar o escopo de tempo, o escopo de tempo padrão será usado.

- Para descobertas, o escopo de tempo padrão usa a primeira e a última vez em que a atividade da descoberta foi observada.
- Para entidades, o escopo de tempo padrão são as 24 horas anteriores.

A seguir, o exemplo de um URL do Detective:

```
https://console.aws.amazon.com/detective/home?region=us-east-1#entities/  
IpAddress/192.168.1.1?scopeStart=1552867200&scopeEnd=1552910400
```

Esse exemplo de URL fornece as instruções a seguir.

- Exiba o perfil da entidade para o endereço IP 192.168.1.
- Use um escopo de tempo que comece na segunda-feira, 18 de março de 2019, às 00:00:00 GMT, e que termine na segunda-feira, 18 de março de 2019, às 12:00:00 GMT.

Solução de problemas de URL

Se o URL não exibir o perfil esperado, primeiro verifique se o URL usa o formato correto e se você forneceu os valores corretos.

- Você começou com o URL correto (`findings` ou `entities`)?
- Você especificou o namespace correto?
- Você forneceu o identificador correto?

Se os valores estiverem corretos, você também poderá verificar o seguinte.

- A descoberta ou a entidade pertence a uma conta-membro habilitada em seu gráfico de comportamento? Se a conta associada não tiver sido convidada para o gráfico de comportamento como uma conta-membro, o gráfico de comportamento não conterá dados dessa conta.

Se uma conta-membro convidada não tiver aceitado o convite, o gráfico de comportamento não conterá dados dessa conta.

- Para uma descoberta, a descoberta está arquivada? Detective não recebe descobertas arquivadas da Amazon. GuardDuty
- A descoberta ou a entidade ocorreu antes de o Detective iniciar a ingestão de dados em seu gráfico de comportamento? Se a descoberta ou entidade não estiver presente nos dados que o Detective ingeriu, o gráfico de comportamento não conterá os dados dela.
- A descoberta ou a entidade é da região correta? Cada gráfico de comportamento é específico de uma região. Um gráfico de comportamento não contém dados de outras regiões.

Adicionar URLs do Detective para descobertas ao Splunk

O projeto Splunk Trumpet permite que você envie dados de AWS serviços para a Splunk.

Você pode configurar o projeto Trumpet para gerar URLs de Detective para descobertas da Amazon GuardDuty. Você também pode usar esses URLs para migrar diretamente do Splunk para os correspondentes perfis de descobertas do Detective.

O projeto Trumpet está disponível no GitHub em <https://github.com/splunk/splunk-aws-project-trumpet>

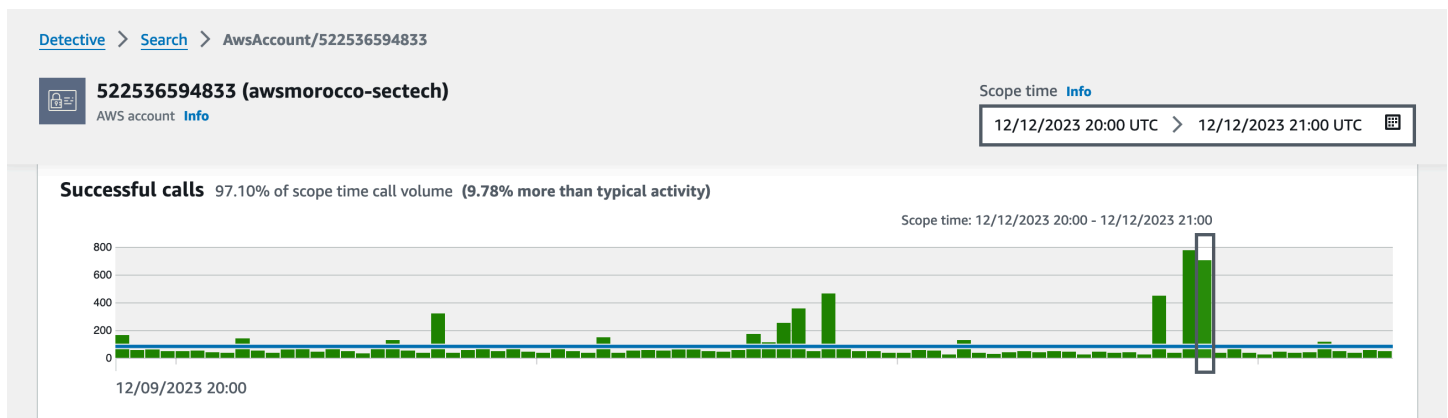
Na página de configuração do projeto Trumpet, em AWS CloudWatch Eventos, escolha Detective URLs. GuardDuty

Navegar por um perfil

O perfil de uma entidade contém um conjunto de uma ou mais guias. Cada guia contém um ou mais painéis de perfil. Cada painel de perfil contém texto e visualizações que são gerados a partir dos dados do gráfico de comportamento.

Conforme você rola para baixo na guia do perfil, as seguintes informações permanecem visíveis na parte superior do perfil:

- Tipo de entidade
- Identificador da entidade
- Escopo de tempo



Gerenciar o escopo de tempo

Personalize o escopo de tempo usado para limitar os dados exibidos nos perfis de entidades.

Os gráficos, cronogramas e outros dados exibidos nos perfis de entidades são todos baseados no escopo de tempo atual. O escopo de tempo é o resumo da atividade de uma entidade ao longo do

tempo. Essa informação aparece no canto superior direito de cada perfil no console do Amazon Detective. Os dados exibidos nesses gráficos, cronogramas e outras visualizações são baseados no escopo de tempo. Para alguns painéis de perfil, um tempo adicional é adicionado antes e depois do escopo de tempo para fornecer contexto. No Detective, todos os carimbos de data/hora são exibidos em UTC por padrão. Você pode selecionar seu fuso horário local alterando as Preferências do carimbo de data/hora. Para atualizar a Preferência de carimbo de data/hora, consulte [the section called “Definir o formato do carimbo de data/hora”](#).

As análises do Detective usam o escopo de tempo ao verificar atividades incomuns. O processo de análise obtém a atividade durante o escopo de tempo e a compara à atividade durante os 45 dias anteriores ao escopo de tempo. Também usa esse período de 45 dias para gerar linhas de base de atividade.

Na visão geral de uma descoberta, o escopo de tempo reflete a primeira e a última vez em que a descoberta foi observada. Para obter mais informações sobre a visão geral de uma descoberta, consulte [the section called “Visão geral da descoberta”](#).

Ao realizar uma investigação, você pode ajustar o escopo de tempo. Por exemplo, se a análise original se baseou na atividade de um único dia, você pode expandi-la para uma semana ou um mês. O período expandido pode ajudá-lo a ter uma ideia melhor sobre se a atividade se encaixa em um padrão normal ou é incomum.

Você também pode definir o escopo de tempo para corresponder uma descoberta associada à entidade atual.

Ao alterar o escopo de tempo, o Detective repete sua análise e atualiza os dados exibidos com base no novo escopo de tempo.

O escopo de tempo não pode ser menor do que uma hora nem maior do que um ano. O horário de início e o horário de término devem ser em uma hora.

Definir datas e horários de início e de término específicos

Você pode definir as datas de início e término do escopo de tempo no console do Detective.

Para definir horários de início e término específicos do novo escopo de tempo

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No perfil de uma entidade, escolha o escopo de tempo.

3. No painel Editar escopo de tempo, em Início, escolha a nova data e hora de início do escopo de tempo. Para o novo horário de início, você escolhe somente a hora.
4. Em Término, escolha a nova data e hora de término do escopo de tempo. Para o novo horário de término, você escolhe somente a hora. O horário de término deve ser pelo menos uma hora depois do horário de início.
5. Ao terminar de editar, para salvar as alterações e atualizar os dados exibidos, escolha Atualizar escopo de tempo.

Editar a duração do escopo de tempo

Ao definir a duração do escopo de tempo, o Detective define o escopo de tempo para essa quantidade de tempo a partir da hora atual.

Para editar a duração do escopo de tempo

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No perfil de uma entidade, escolha o escopo de tempo.
3. No painel Editar escopo de tempo, ao lado de Histórico, escolha a duração do escopo de tempo.

A especificação de um intervalo de tempo atualiza as configurações de Início e Término.

4. Ao terminar de editar, para salvar as alterações e atualizar os dados exibidos, escolha Atualizar escopo de tempo.

Definir o escopo de tempo para a janela de tempo de uma descoberta

Cada descoberta tem uma janela de tempo associada, que reflete a primeira e a última vez em que a descoberta foi observada. Ao visualizar a visão geral de uma descoberta, o escopo de tempo muda para a janela de tempo da descoberta.

No perfil de uma entidade, você pode alinhar o escopo de tempo à janela de tempo de uma descoberta associada. Isso permite que você investigue a atividade que ocorreu durante esse período.

Para alinhar o escopo de tempo à janela de tempo de uma descoberta, no painel Descobertas associadas, escolha a descoberta que você deseja usar.

O Detective preenche os detalhes da descoberta e define o escopo de tempo para a janela de tempo da descoberta.

Definir o escopo de tempo na página Resumo

Ao revisar a página Resumo, você pode ajustar o escopo de tempo para visualizar a atividade em qualquer período de 24 horas nos últimos 365 dias.

Para definir o escopo de tempo na página Resumo

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, escolha Resumo.
3. No painel Escopo de tempo, ao lado de Resumo, você pode alterar a Data e hora de início. A hora de início deve estar nos últimos 365 dias.

Ao alterar a Data e hora de início, a Data e hora de término é atualizada automaticamente para 24 horas após a hora de início escolhida.

Note

Com o Detective, você pode acessar até um ano de dados do histórico de eventos. Para obter mais informações sobre os dados de origem no Detective, consulte [Dados de origem usados em um gráfico de comportamento](#).

4. Ao terminar de editar, para salvar as alterações e atualizar os dados exibidos, escolha Atualizar escopo de tempo.

Visualizar detalhes das descobertas associadas

Cada perfil de entidade contém um painel de descobertas associadas que lista as descobertas que envolveram a entidade durante o escopo de tempo atual. Uma indicação de que uma entidade foi comprometida é seu envolvimento em várias descobertas. Os tipos de descobertas também podem fornecer informações sobre o tipo de atividade com a qual se preocupar.

O painel de descobertas associadas é exibido imediatamente abaixo do painel de perfil de detalhes da entidade.

Para cada descoberta, a tabela inclui as seguintes informações:

- O título da descoberta, que também é um link para a visão geral da descoberta.
- A AWS conta associada à descoberta, que também é um link para o perfil da conta
- O tipo da descoberta.
- A primeira vez em que a descoberta foi observada.
- A última vez em que a descoberta foi observada.
- A severidade da descoberta.

Para exibir os detalhes da descoberta, escolha o botão de opção da descoberta. O Detective preenche o painel de detalhes da descoberta à direita da página. Também altera o escopo de tempo para ser a janela de tempo da descoberta. Isso permite que você se concentre nas atividades que ocorreram durante esse período.

Se você navegou até o perfil da entidade a partir da visão geral de uma descoberta, essa descoberta será selecionada automaticamente e seus detalhes serão exibidos.

Nos detalhes da descoberta, para voltar à visão geral, escolha Ver todas as entidades relacionadas.

Você também pode arquivar a descoberta. Consulte [the section called “Arquivando uma descoberta GuardDuty”](#).

Visualizar detalhes de entidades de alto volume

No [gráfico de comportamento](#), o Amazon Detective rastreia os relacionamentos entre entidades. Por exemplo, cada gráfico de comportamento rastreia quando um AWS usuário cria uma AWS função e quando uma instância do EC2 se conecta a um endereço IP.

Quando uma entidade tem muitos relacionamentos durante um período de tempo, o Detective não pode armazenar todos os relacionamentos. Quando isso ocorre durante o escopo de tempo atual, o Detective notifica você. O Detective também fornece uma lista de ocorrências de entidades de alto volume.

O que é uma entidade de alto volume?

Durante um determinado intervalo de tempo, uma entidade pode ser a origem ou o destino de um número extremamente grande de conexões. Por exemplo, uma instância do EC2 pode ter conexões a partir de milhões de endereços IP.

O Detective mantém um limite no número de conexões que ele pode acomodar durante cada intervalo de tempo. Se uma entidade exceder esse limite, o Detective descarta as conexões desse intervalo de tempo.

Por exemplo, suponha que o limite seja de 100.000.000 de conexões por intervalo de tempo. Se uma instância do EC2 for conectada a mais de 100.000.000 de endereços IP durante um intervalo de tempo, o Detective descartará as conexões desse intervalo de tempo.

No entanto, talvez você consiga analisar essa atividade com base na entidade do outro lado do relacionamento. Para continuar o exemplo, embora uma instância do EC2 possa estar conectada a partir de milhões de endereços IP, um único endereço IP se conecta a muito menos instâncias do EC2. Cada perfil de endereço IP fornece detalhes sobre as instâncias do EC2 às quais o endereço IP está conectado.

Visualizar a notificação de entidade de alto volume em um perfil

O Detective exibe um aviso na parte superior de uma descoberta ou de um perfil de entidade se o escopo de tempo incluir um intervalo de tempo em que a entidade tiver alto volume. Para os perfis de descobertas, o aviso é para a entidade envolvida.

O aviso inclui a lista de relacionamentos com intervalos de tempo de alto volume. Cada entrada da lista contém uma descrição do relacionamento e o início do intervalo de tempo de alto volume.

Um intervalo de tempo de alto volume pode ser um indicador de atividade suspeita. Para entender quais outras atividades ocorreram ao mesmo tempo, você pode concentrar sua investigação em um intervalo de tempo de alto volume. O aviso de entidade de alto volume inclui uma opção para definir o escopo de tempo para esse intervalo de tempo.

Para definir o escopo de tempo para um intervalo de tempo de alto volume

1. No aviso de entidade de alto volume, escolha o intervalo de tempo.
2. No menu pop-up, escolha Aplicar escopo de tempo.

Visualizar a lista de entidades de alto volume para o escopo de tempo atual

A página Entidades de alto volume contém uma lista de intervalos de tempo e entidades de alto volume durante o escopo de tempo atual.

Para exibir a página de entidades de alto volume

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, escolha Entidades de alto volume.

Cada item da lista contém as seguintes informações:

- O início do intervalo de tempo de alto volume
- O identificador e o tipo de entidade
- A descrição do relacionamento, tal como “instância do EC2 conectada a partir do endereço IP”

É possível filtrar e ordenar a lista por qualquer uma das colunas. Você também pode navegar até o perfil da entidade envolvida.

Para navegar até o perfil de uma entidade

1. Na lista de Entidades de alto volume, escolha a linha a partir da qual navegar.
2. Escolha Visualizar perfil com escopo de tempo de alto volume.

Quando você usa essa opção para navegar até o perfil de uma entidade, o escopo de tempo é definido da seguinte forma:

- O escopo de tempo começa 30 dias antes do intervalo de tempo de alto volume.
- O escopo de tempo termina no final do intervalo de tempo de alto volume.

Gerenciando descobertas e entidades

O Amazon Detective oferece vários recursos importantes para ajudar você a pesquisar, exportar e gerenciar suas descobertas. Esses recursos ajudarão você a adaptar as descobertas ao seu ambiente específico, reduzir o ruído de descobertas de baixo valor e ajudá-lo a se concentrar nas ameaças ao seu AWS ambiente exclusivo. Analise os tópicos desta página para entender como você pode usar esses recursos para aumentar o valor das descobertas do Detective.

Conteúdo

- [Procurar por uma descoberta ou entidade](#)
- [Exportar dados do Detective](#)
- [Arquivando uma descoberta da Amazon GuardDuty](#)

Procurar por uma descoberta ou entidade

Com a função de pesquisa do Amazon Detective, você pode pesquisar uma descoberta ou entidade. A partir dos resultados da pesquisa, você pode navegar até o perfil de uma entidade ou até a visão geral de uma descoberta. Se sua pesquisa retornar mais de 10.000 resultados, somente os 10.000 primeiros resultados serão exibidos. Mudar a ordem de classificação altera os resultados retornados.

Você pode exportar os resultados da pesquisa para um arquivo de valores separados por vírgulas (CSV). Esse arquivo contém os dados retornados na página de pesquisa. Para ter mais informações, consulte [the section called “Exportar dados do Detective”](#).

Concluir a pesquisa

Para concluir a pesquisa, escolha o tipo de entidade a ser pesquisada. Em seguida, forneça o identificador exato ou o identificador com os caracteres curinga * ou ?. Para pesquisar por um intervalo de endereços IP, você também pode usar notações CIDR ou de pontos. Veja a seguir um exemplo de sequência de caracteres de pesquisa.

Para endereços IP:

- 1.0.*.*
- 1.0.133.*
- 1.0.0.0/16

- 0.239.48.198/31

Para todos os outros tipos de entidade:

- Admin
- ad*
- ad*n
- ad*n*
- adm?n
- a?m*
- *min

Para cada tipo de entidade, os seguintes identificadores são compatíveis:

- Para descobertas, o identificador da descoberta ou o nome do recurso da Amazon (ARN).
- Para AWS contas, o ID da conta.
- Para AWS funções e AWS usuários, o ID principal, o nome ou o ARN.
- Para clusters de contêiner, o nome do cluster ou o ARN.
- Para imagens de contêiner, o repositório ou o resumo completo da imagem de contêiner.
- Para pods ou tarefas de contêiner, o nome do pod ou o UID do pod.
- Para instâncias do EC2, o identificador da instância ou o ARN.
- Para grupos de descoberta, o identificador do grupo de descoberta.
- Para endereços IP, o endereço em notação CIDR ou de pontos.
- Para sujeitos do Kubernetes (contas de serviço ou usuários), o nome.
- Para uma sessão de função, você pode usar qualquer um dos valores a seguir para pesquisar:
 - O identificador da sessão de função.

O identificador da sessão de função usa o formato *<rolePrincipalID>:<sessionName>*.

Aqui está um exemplo: AR0A12345678910111213:MySession.

- ARN da sessão de função
- Nome da sessão
- ID da entidade principal da função que foi assumida

- Nome da função que foi assumida
- Para buckets do S3, o nome do bucket ou o ARN do bucket.
- Para usuários federados, a ID da entidade principal ou o nome de usuário.
O ID da entidade principal é `<identityProvider>:<username>` ou `<identityProvider>:<audience>:<username>`.
- Para agentes de usuário, o nome do agente de usuário.

Para pesquisar por uma descoberta ou entidade

1. Faça login no AWS Management Console. Em seguida, abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, selecione Pesquisar.
3. No menu Escolher tipo, escolha o tipo de item que você está procurando.

Observe que, ao escolher Usuário, você pode pesquisar um usuário da AWS ou um usuário federado.

A opção Exemplos de seus dados contém um conjunto de amostras de identificadores do tipo selecionado que estão nos dados do gráfico de comportamento. Para exibir o perfil de um dos exemplos, escolha seu identificador.

4. Insira o identificador exato ou um identificador com caracteres curinga para pesquisar.

A pesquisa não diferencia maiúsculas de minúsculas.

5. Escolha Pesquisar ou pressione Enter.

Usar os resultados da pesquisa

Quando você conclui a pesquisa, o Detective exibe uma lista de até 10.000 resultados correspondentes. Para pesquisas que usam um identificador exclusivo, há apenas um resultado correspondente.

Nos resultados, para navegar até o perfil da entidade ou a visão geral da descoberta, escolha o identificador.

Para descobertas, funções, usuários e instâncias do EC2, os resultados da pesquisa incluem a conta associada. Para navegar até o perfil da conta, escolha o identificador da conta.

Solucionar problemas da pesquisa

Se o Detective não encontrar a descoberta ou a entidade, primeiro verifique se você inseriu o identificador correto. Se o identificador estiver correto, você também pode verificar o seguinte.

- A descoberta ou a entidade pertence a uma conta-membro habilitada em seu gráfico de comportamento? Se a conta associada não tiver sido convidada para o gráfico de comportamento como uma conta-membro, o gráfico de comportamento não conterá dados dessa conta.

Se uma conta-membro convidada não tiver aceitado o convite, o gráfico de comportamento não conterá dados dessa conta.

- Para uma descoberta, a descoberta está arquivada? Detective não recebe descobertas arquivadas da Amazon. GuardDuty
- A descoberta ou a entidade ocorreu antes de o Detective iniciar a ingestão de dados em seu gráfico de comportamento? Se a descoberta ou entidade não estiver presente nos dados que o Detective ingeriu, o gráfico de comportamento não conterá os dados dela.
- A descoberta ou a entidade é da região correta? Cada gráfico de comportamento é específico para um Região da AWS. Um gráfico de comportamento não contém dados de outras regiões.

Exportar dados do Detective

Você pode exportar dados da página Resumo do Amazon Detective e da página de resultados de pesquisa. Os dados são exportados no formato CSV (valores separados por vírgula). O nome do arquivo dos dados exportados segue o formato padrão `detective-page-panel-yyyy-mm-dd.csv`. Você pode enriquecer suas investigações de segurança ao manipular os dados usando outros serviços da AWS, aplicativos de terceiros ou programas de planilhas que oferecem suporte à importação de CSV.

Note

Se uma exportação estiver em andamento, aguarde até que seja concluída antes de tentar exportar dados adicionais.

É possível exportar um arquivo .csv (valores separados por vírgula) contendo os dados dos seguintes painéis e páginas no Detective:

- **Página Resumo**
 - Painel Funções e usuários com o maior volume de chamadas de API
 - Painel Instâncias do EC2 com o maior volume de tráfego
 - Painel Clusters do EKS com o maior número de pods do Kubernetes criados
- **Página Pesquisar:** se sua pesquisa retornar mais de 10.000 resultados, somente os 10.000 primeiros resultados serão exportados. Mudar a ordem de classificação altera os resultados retornados.

Arquivando uma descoberta da Amazon GuardDuty

Ao concluir sua investigação sobre uma GuardDuty descoberta da Amazon, você pode arquivá-la com o Amazon Detective. Isso evita que você precise voltar para GuardDuty fazer a atualização. Arquivar uma descoberta indica que você concluiu sua investigação.

Você só pode arquivar uma GuardDuty descoberta de dentro do Detective se você também for a conta de GuardDuty administrador da conta associada à descoberta. Se você não for uma conta de GuardDuty administrador e tentar arquivar uma descoberta, GuardDuty exibirá um erro.

Para arquivar uma GuardDuty descoberta

1. No console do Detective, no painel de detalhes da descoberta, escolha Arquivar descoberta.
2. Quando for solicitada sua confirmação, escolha Arquivar.

Você pode ver as GuardDuty descobertas arquivadas no GuardDuty console. Para saber mais, consulte [Regras de supressão](#) no Guia do GuardDuty usuário da Amazon.

Gerenciar contas

Cada gráfico de comportamento contém dados de uma ou mais contas. Quando uma conta habilita o Detective, ela se torna a conta de administrador do gráfico de comportamento e escolhe as contas-membro do gráfico de comportamento. Um gráfico de comportamento pode ter até 1.200 contas-membro.

Se você estiver integrado com AWS Organizations, a conta de gerenciamento da organização designará a conta de administrador do Detective para a organização. Essa conta de administrador do Detective se torna a conta de administrador do gráfico de comportamento da organização. A conta de administrador do Detective pode habilitar quaisquer contas da organização como contas-membro no gráfico de comportamento da organização. As contas da organização não podem se remover do gráfico de comportamento da organização.

Uma conta de administrador também pode convidar contas para participar de um gráfico de comportamento. Quando a conta aceita o convite, o Detective habilita a conta como uma conta-membro. As contas-membro que são adicionadas por convite podem se remover do gráfico de comportamento.

Quando uma conta é habilitada como conta-membro, o Detective começa a ingestão e extração dos dados da conta-membro para esse gráfico de comportamento.

O Detective cobra de cada conta pelos dados que contribui para cada gráfico de comportamento. Para obter informações sobre como rastrear o volume de dados de cada conta em um gráfico de comportamento, consulte [Previsão e monitoramento dos custos do Amazon Detective](#).

Conteúdo

- [Restrições e recomendações de conta no Detective](#)
- [Transição para usar o Organizations no gerenciamento de contas em gráficos de comportamento](#)
- [Designar a conta de administrador do Detective para uma organização](#)
- [Ações disponíveis para contas](#)
- [Visualizar a lista de contas](#)
- [Gerenciar contas da organização como contas-membro](#)
- [Gerenciar contas-membro convidadas](#)
- [Para contas-membro: gerenciar convites e associações a gráficos de comportamento](#)

- [Efeito das ações da conta nos gráficos de comportamento](#)
- [Usando os scripts do Amazon Detective Python para gerenciar contas](#)

Restrições e recomendações de conta no Detective

Ao gerenciar contas no Amazon Detective, preste atenção às restrições e recomendações a seguir.

Número máximo de contas-membro

O Detective permite até 1.200 contas-membro em cada gráfico de comportamento.

Contas e regiões

Se você usa AWS Organizations para gerenciar contas, a conta de gerenciamento da organização designa uma conta de administrador de Detective para a organização. A conta de administrador do Detective se torna a conta de administrador do gráfico de comportamento da organização.

A conta de administrador do Detective deve ser a mesma em todas as regiões. A conta de gerenciamento da organização designa a conta de administrador do Detective separadamente em cada região. A conta de administrador do Detective também gerencia os gráficos de comportamento e as contas-membro da organização separadamente em cada região.

Para contas-membro criadas por convite, a associação administrador-membro é criada somente na região de onde o convite é enviado. A conta de administrador deve habilitar o Detective em cada região e ter um gráfico de comportamento separado em cada região. A conta de administrador convida cada conta a se associar como uma conta-membro nessa região.

Uma conta pode ser uma conta-membro de vários gráficos de comportamento na mesma região. Uma conta só pode ser a conta de administrador de um gráfico de comportamento por região. Uma conta pode ser uma conta de administrador em diferentes regiões.

Alinhamento das contas de administrador com o Security Hub e GuardDuty

Para garantir que as integrações com AWS Security Hub e Amazon GuardDuty funcionem sem problemas, recomendamos que a mesma conta seja a conta de administrador em todos esses serviços.

Consulte [the section called “Alinhamento recomendado com e GuardDuty AWS Security Hub”](#).

Conceder as permissões necessárias para contas de administrador

Para garantir que uma conta de administrador tenha as permissões necessárias para gerenciar seu gráfico de comportamento, anexe a [política gerenciada AmazonDetectiveFullAccess](#) à entidade principal do IAM.

Refletir as atualizações da organização no Detective

As mudanças em uma organização não são refletidas imediatamente no Detective.

Para a maioria das mudanças, como contas organizacionais novas e removidas, pode levar até uma hora para que o Detective seja notificado.

Uma mudança na conta designada como administrador do Detective no Organizations leva menos tempo para ser propagada.

Transição para usar o Organizations no gerenciamento de contas em gráficos de comportamento

Você pode já ter um gráfico de comportamento com contas-membro que aceitaram um convite manual. Se você estiver inscrito AWS Organizations, use as etapas a seguir para usar o Organizations para habilitar e gerenciar contas de membros em vez de usar o processo de convite manual:

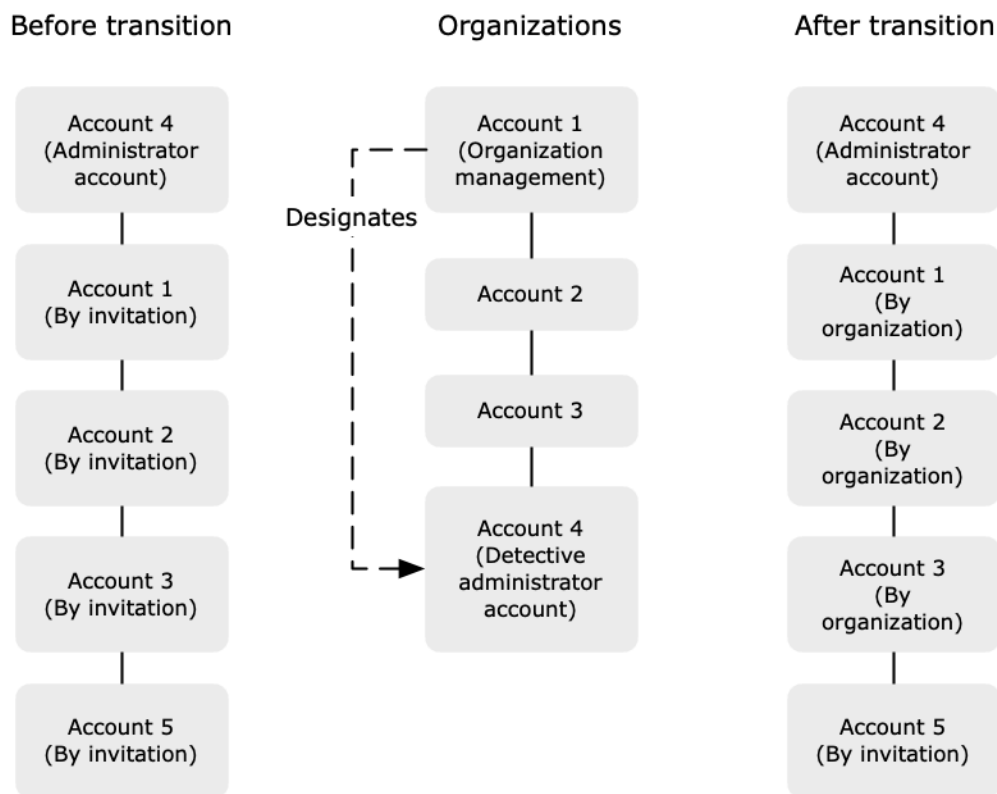
1. [Designar a conta de administrador do Detective para a organização.](#) Isso cria o gráfico de comportamento da organização.

Se a conta de administrador do Detective já tiver um gráfico de comportamento, esse gráfico se torna o gráfico de comportamento da organização.

2. [Habilitar contas da organização como contas-membro no gráfico de comportamento da organização.](#)

Se o gráfico de comportamento da organização tiver contas-membro existentes que sejam contas da organização, essas contas são habilitadas automaticamente.

O diagrama a seguir mostra uma visão geral da estrutura do gráfico de comportamento antes da transição, da configuração no Organizations e da estrutura da conta no gráfico de comportamento após a transição.



Designar a conta de administrador do Detective para a organização

A conta de gerenciamento da organização designa a conta de administrador do Detective para a organização. Consulte [the section called “Designar a conta de administrador do Detective”](#).

Para simplificar a transição, o Detective recomenda que você escolha uma conta de administrador atual como a conta de administrador do Detective da organização.

Se houver uma conta de administrador delegado para o Detective no Organizations, você deve usar essa conta ou a conta de gerenciamento da organização como a conta de administrador do Detective.

Caso contrário, na primeira vez que você designar uma conta de administrador de Detective que não seja a conta de gerenciamento da organização, o Detective sinaliza para o Organizations para transformar essa conta na conta de administrador delegado do Detective.

Habilitar contas da organização como contas-membro

A conta de administrador do Detective é a conta de administrador do gráfico de comportamento da organização. A conta de administrador do Detective escolhe as contas da organização para serem

habilitadas como contas-membro no gráfico de comportamento da organização. Consulte [the section called “Gerenciar contas-membro da organização”](#).

Na página Contas, a conta de administrador do Detective vê todas as contas da organização.

Se a conta de administrador do Detective já for a conta de administrador do gráfico de comportamento, esse gráfico se torna o gráfico de comportamento da organização. Contas da organização que já eram contas-membro desse gráfico de comportamento são habilitadas como contas-membro automaticamente. Outras contas da organização têm o status Não é membro.

As contas da organização têm o tipo Por organização, mesmo que tenham sido anteriormente contas-membro convidadas.

As contas-membro que não pertencem à organização têm o tipo Por convite.

A página Gerenciamento de contas também fornece uma opção, Habilitar automaticamente novas contas da organização, para habilitar automaticamente novas contas à medida que são adicionadas a uma organização. Consulte [the section called “Habilitar novas contas da organização automaticamente”](#). A opção está inicialmente desabilitada.

Quando a conta de administrador do Detective exibe pela primeira vez a página Gerenciamento de contas, ela exibe uma mensagem contendo o botão Habilitar todas as contas da organização. Ao escolher Habilitar todas as contas da organização, o Detective executa as seguintes ações:

- Habilita todas as contas atuais da organização como contas-membro.
- Habilita a opção de habilitar novas contas-membro da organização automaticamente.

Também há a opção Habilitar todas as contas da organização na lista de contas-membro.

Designar a conta de administrador do Detective para uma organização

No gráfico de comportamento da organização, a conta de administrador do Detective gerencia a associação ao gráfico de comportamento de todas as contas da organização.

Como a conta de administrador do Detective é gerenciada

A conta de gerenciamento da organização designa a conta de administrador do Detective para a organização em cada uma. Região da AWS

Configurar a conta de administrador do Detective como a conta de administrador delegado

A conta de administrador do Detective também se torna a conta de administrador delegado do Detective in. AWS Organizations A exceção é se a conta de gerenciamento da organização designa a si própria como a conta de administrador do Detective. A conta de gerenciamento da organização não pode ser um administrador delegado no Organizations.

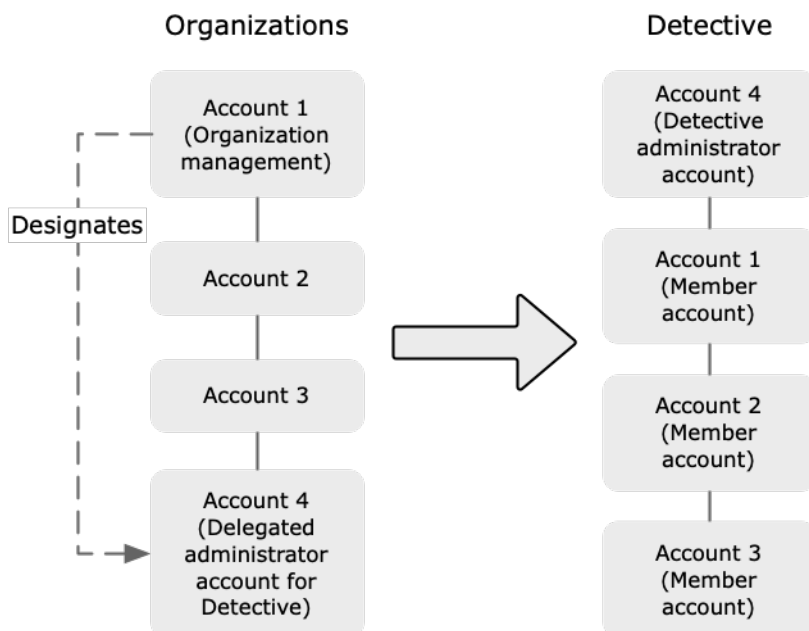
Após a conta de administrador delegado ser definida no Organizations, a conta de gerenciamento da organização só pode escolher a conta de administrador delegado ou sua própria conta como conta de administrador do Detective. Recomendamos que você escolha a conta de administrador delegado em todas as regiões.

Criar e gerenciar o gráfico de comportamento da organização

Quando a conta de gerenciamento da organização escolhe uma conta de administrador do Detective, o Detective cria um novo gráfico de comportamento para essa conta. Esse gráfico é o gráfico de comportamento da organização.

Se a conta de administrador do Detective for uma conta de administrador para um gráfico de comportamento existente, esse gráfico se tornará o gráfico de comportamento da organização.

A conta de administrador do Detective escolhe as contas da organização para serem habilitadas como contas-membro no gráfico de comportamento da organização.



A conta de administrador do Detective também pode enviar convites para contas que não pertencem à organização. Para obter mais informações, consulte [the section called “Gerenciar contas-membro da organização”](#) e [the section called “Gerenciar contas convidadas”](#).

Remover a conta de administrador do Detective

A conta de gerenciamento da organização pode remover a conta de administrador atual do Detective em uma região. Ao remover a conta de administrador do Detective, o Detective só a remove da região atual. Isso não altera a conta de administrador delegado no Organizations.

Quando a conta de gerenciamento da organização remove a conta de administrador do Detective em uma região, o Detective exclui o gráfico de comportamento da organização. O Detective é desabilitado da conta de administrador do Detective removida.

Para remover a atual conta de administrador delegado do Detective, use a API do Organizations. Ao remover a conta de administrador delegado do Detective no Organizations, o Detective exclui todos os gráficos de comportamento da organização em que a conta de administrador delegado é a conta de administrador do Detective. Os gráficos de comportamento da organização cuja conta de gerenciamento da organização é a conta de administrador do Detective não são afetados.

Permissões necessárias para configurar a conta de administrador do Detective

Para garantir que a conta de gerenciamento da organização possa configurar a conta de administrador do Detective, você pode anexar a [política gerenciada do AmazonDetectiveOrganizationsAccess](#) às suas entidades do AWS Identity and Access Management (IAM).

Designar uma conta de administrador do Detective (console)

A conta de gerenciamento da organização pode usar o console do Detective para designar a conta de administrador do Detective.

Não é necessário habilitar o Detective para gerenciar a conta de administrador do Detective. Você pode gerenciar a conta de administrador do Detective na página [Habilitar o Detective](#).

Para designar uma conta de administrador do Detective (página [Habilitar o Detective](#))

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.

2. Escolha Comece a usar.
3. No painel Permissões necessárias para contas de administrador, conceda as permissões necessárias à conta que você escolher para que ela possa operar como administradora do Detective, com acesso total a todas as ações no Detective. Para operar como administrador, recomendamos anexar a política `AmazonDetectiveFullAccess` à entidade principal.
4. Escolha Anexar política do IAM para visualizar a política recomendada diretamente no console do IAM.
5. Dependendo se você tem permissões no console do IAM, faça o seguinte:
 - Se você tem permissões para operar no console do IAM, anexe a política recomendada à entidade principal que você usa para o Detective.
 - Se você não tem permissões para operar no console do IAM, copie o nome do recurso da Amazon (ARN) da política e forneça-o ao administrador do IAM. A política poderá então ser anexada em seu nome.
6. Em Administrador delegado, escolha a conta de administrador do Detective.

As opções disponíveis dependem de você ter uma conta de administrador delegado do Detective no Organizations.

- Se você não tiver uma conta de administrador delegado do Detective no Organizations, insira o identificador da conta para designá-la como a conta de administrador do Detective.

Você pode obter uma conta de administrador existente e um gráfico de comportamento pelo processo de convite manual. Nesse caso, recomendamos que você designe essa conta como a conta de administrador do Detective.

Se você tiver uma conta de administrador delegada no Organizations for Amazon ou no Amazon Macie GuardDuty AWS Security Hub, o Detective solicitará que você selecione uma dessas contas. Você também pode inserir uma conta diferente.

- Se você tem uma conta de administrador delegado do Detective no Organizations, deverá escolher essa conta ou sua conta. Recomendamos que você escolha a conta de administrador delegado em todas as regiões.

7. Escolha Delegar.

Se você tiver o Detective habilitado ou for uma conta-membro em um gráfico de comportamento existente, poderá designar a conta de administrador do Detective na página Geral.

Para designar uma conta de administrador do Detective (página Geral)

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, em Configurações, selecione Geral.
3. No painel Políticas gerenciadas, você pode aprender mais sobre todas as políticas gerenciadas compatíveis com o Detective. Você pode conceder as permissões necessárias a uma conta, dependendo das ações que você deseja que os usuários realizem no Detective. Para operar como administrador, recomendamos anexar a política AmazonDetectiveFullAccess à entidade principal.
4. Dependendo se você tem permissões no console do IAM, faça o seguinte:
 - Se você tem permissões para operar no console do IAM, anexe a política recomendada à entidade principal que você usa para o Detective.
 - Se você não tem permissões para operar no console do IAM, copie o nome do recurso da Amazon (ARN) da política e forneça-o ao administrador do IAM. A política poderá então ser anexada em seu nome.

As opções disponíveis dependem de você ter uma conta de administrador delegado do Detective no Organizations.

- Se você não tiver uma conta de administrador delegado do Detective no Organizations, insira o identificador da conta para designá-la como a conta de administrador do Detective.

Você pode obter uma conta de administrador existente e um gráfico de comportamento pelo processo de convite manual. Nesse caso, recomendamos que você designe essa conta como a conta de administrador do Detective.

Se você tiver uma conta de administrador delegada no Organizations for Amazon ou no Amazon Macie GuardDuty AWS Security Hub, o Detective solicitará que você selecione uma dessas contas. Você também pode inserir uma conta diferente.

- Se você tem uma conta de administrador delegado do Detective no Organizations, deverá escolher essa conta ou sua conta. Recomendamos que você escolha a conta de administrador delegado em todas as regiões.
5. Escolha Delegar.

Designar uma conta de administrador do Detective (API do Detective, AWS CLI)

Para designar a conta de administrador do Detective, você pode usar uma chamada de API ou a AWS Command Line Interface. Você deve usar as credenciais da conta de gerenciamento da organização.

Se você já tem uma conta de administrador delegado do Detective no Organizations, então você deve escolher essa conta ou sua conta. Recomendamos que você escolha a conta de administrador delegado.

Para designar a conta de administrador do Detective (Detective API,) AWS CLI

- API do Detective: use a operação [EnableOrganizationAdminAccount](#). Você deve fornecer o identificador de conta da AWS da conta de administrador do Detective. Para obter o identificador da conta, use a operação [ListOrganizationAdminAccounts](#).
- AWS CLI: na linha de comando, execute o comando [enable-organization-admin-account](#).

```
aws detective enable-organization-admin-account --account-id <admin account ID>
```

Exemplo

```
aws detective enable-organization-admin-account --account-id 777788889999
```

Remover uma conta de administrador do Detective (console)

No console do Detective, você pode remover a conta de administrador do Detective.

Quando a conta de administrador do Detective é removida, o Detective é desabilitado para a conta e o gráfico de comportamento da organização é excluído. A conta de administrador do Detective é removida apenas na região atual.

Important

A remoção de uma conta de administrador do Detective não afeta a conta de administrador delegado no Organizations.

Para remover a conta de administrador do Detective (página Habilitar Detective)

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. Escolha Comece a usar.
3. Em Administrador delegado, escolha Desabilitar Amazon Detective.
4. Na caixa de diálogo de confirmação, insira **disable** e escolha Desabilitar Amazon Detective.

Para remover uma conta de administrador do Detective (página Geral)

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, em Configurações, selecione Geral.
3. Em Administrador delegado, escolha Desabilitar Amazon Detective.
4. Na caixa de diálogo de confirmação, insira **disable** e escolha Desabilitar Amazon Detective.

Removendo a conta de administrador do Detective (Detective API,) AWS CLI

Para remover a conta de administrador do Detective, você pode usar uma chamada de API ou a AWS CLI. Você deve usar as credenciais da conta de gerenciamento da organização.

Quando a conta de administrador do Detective é removida, o Detective é desabilitado para a conta e o gráfico de comportamento da organização é excluído.

Important

A remoção de uma conta de administrador do Detective não afeta a conta de administrador delegado no Organizations.

Para remover a conta de administrador do Detective (Detective API,) AWS CLI

- API do Detective: use a operação [DisableOrganizationAdminAccount](#).

Quando você usa a API do Detective para remover a conta de administrador do Detective, ela só é removida na região em que a chamada ou o comando da API foi emitido.

- AWS CLI: na linha de comando, execute o comando [disable-organization-admin-account](#).

```
aws detective disable-organization-admin-account
```

Removendo a conta de administrador delegado (Organizations API, AWS CLI)

A remoção de uma conta de administrador do Detective não remove automaticamente a conta de administrador delegado no Organizations. Para remover a conta de administrador delegado do Detective, você pode usar a API do Organizations.

Ao remover a conta de administrador delegado, todos os gráficos de comportamento da organização em que a conta de administrador delegado é a conta de administrador do Detective são excluídos. O Detective da conta nessas regiões também é desabilitado.

Para remover a conta de administrador delegado (Organizations API, AWS CLI)

- API do Organizations: use a operação [DeregisterDelegatedAdministrator](#). Você deve fornecer o identificador da conta de administrador do Detective, além da entidade principal de serviço do Detective, que é `detective.amazonaws.com`.
- AWS CLI: na linha de comando, execute o comando [deregister-delegated-administrator](#).

```
aws organizations deregister-delegated-administrator --account-id <Detective administrator account ID> --service-principal <Detective service principal>
```

Exemplo

```
aws organizations deregister-delegated-administrator --account-id 777788889999 --service-principal detective.amazonaws.com
```

Ações disponíveis para contas

As contas de administrador e contas-membro têm acesso às seguintes ações do Detective. Na tabela, os valores têm os seguintes significados:

- Any – A conta pode realizar a ação para todas as contas na mesma conta de administrador do Detective.

- Self – A conta só pode realizar a ação em sua própria conta.
- Dash (–) – A conta não pode realizar a ação.

No gráfico de comportamento da organização, a conta de administrador do Detective determina as contas da organização para serem habilitadas como contas-membro. O Detective pode ser configurado para habilitar novas contas da organização como contas-membro automaticamente, ou as contas da organização podem ser habilitadas manualmente.

Uma conta de administrador também pode convidar contas para serem contas-membro em um gráfico de comportamento. Quando uma conta-membro aceita o convite e é habilitada, o Amazon Detective começa a ingestão e extração dos dados da conta-membro para esse gráfico de comportamento.

Para gráficos de comportamento que não sejam o da organização, todas as contas-membro são contas convidadas.

A tabela a seguir reflete as permissões padrão para contas de administrador e contas-membro. Você pode usar políticas personalizadas do IAM para restringir ainda mais o acesso aos atributos e funções do Detective.

Ação	Conta de administrador (Organização)	Conta de administrador (Convite)	Membro (Organização)	Membro (Convite)
Visualizar contas	Any	Any	Self (Visualizar contas de administrador)	Self (Visualizar contas de administrador)
Remover conta-membro	Any As contas convidadas são removidas As contas da organização são desassociadas	Any	–	Self

Ação	Conta de administrador (Organização)	Conta de administrador (Convite)	Membro (Organização)	Membro (Convite)
Adicionar ou remover pacotes de fontes de dados opcionais	Any (A configuração se aplica a todas as contas-membro)	Any (A configuração se aplica a todas as contas-membro)	–	–
Desabilitar Detective	Self	Self	–	–
Visualizar dados do gráfico de comportamento	Any	Any	–	–
Habilitar ou desabilitar pacotes de fontes de dados opcionais	Todos	Todos	–	–

Visualizar a lista de contas

A conta de administrador pode usar o console ou a API do Detective para visualizar uma lista de contas. A lista pode incluir:

- Contas convidadas pela conta de administrador para participar do gráfico de comportamento. Essas contas têm o tipo Por convite.
- Para o gráfico de comportamento da organização, todas as contas da organização. Essas contas têm o tipo Por organização.

Os resultados não incluem contas-membro convidadas que recusaram um convite ou que foram removidas do gráfico de comportamento pela conta de administrador. Inclui apenas contas com os status a seguir.

Verificação em andamento

Para contas convidadas, o Detective está verificando o endereço de e-mail da conta antes de enviar o convite.

Para contas da organização, o Detective está verificando se a conta pertence à organização. O Detective também verifica se foi a conta de administrador do Detective que habilitou a conta.

Verificação falhou

A verificação falhou. O convite não foi enviado ou a conta da organização não foi habilitada como membro.

Convidado

Para contas convidadas. O convite foi enviado, mas a conta-membro ainda não respondeu.

Não é membro

Para contas da organização no gráfico de comportamento da organização. Atualmente, a conta da organização não é uma conta-membro. Não contribui com dados para o gráfico de comportamento da organização.

Habilitado

Para contas convidadas, a conta-membro aceitou o convite e contribui com dados para o gráfico de comportamento.

Para contas da organização no gráfico de comportamento da organização, a conta de administrador do Detective a habilitou como conta-membro. A conta contribui com dados para o gráfico de comportamento da organização.

Não habilitado

Para contas convidadas, a conta-membro aceitou o convite, mas não pode ser habilitada.

Para contas da organização no gráfico de comportamento da organização, a conta de administrador do Detective tentou habilitar a conta, mas não pode ser habilitada.

Esse status ocorre por um dos seguintes motivos.

- A conta do membro não é GuardDuty cliente da Amazon há pelo menos 48 horas.
- Os dados da conta-membro fariam com que o volume de dados do gráfico de comportamento excedesse a cota do Detective.

Listar contas (Console)

Você pode usar o AWS Management Console para ver e filtrar sua lista de contas.

Para exibir a lista de contas (console)

1. Faça login no AWS Management Console. Em seguida, abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, escolha Gerenciamento de contas.

A lista de contas-membro contém as seguintes contas:

- Sua conta
- Contas que você convidou para contribuir com dados no gráfico de comportamento
- No gráfico de comportamento da organização, todas as contas da organização

Para cada conta, a lista exibe as seguintes informações:

- O identificador AWS da conta.
- Para contas da organização, o nome da conta.
- O tipo de conta (Por convite ou Por organização).
- Para contas convidadas, o endereço de e-mail do usuário raiz da conta.
- O status da conta.
- O volume diário de dados da conta. O Detective não consegue recuperar o volume de dados de contas que não estão habilitadas como contas-membro.
- A data em que o status da conta foi atualizado pela última vez.

Você pode usar as guias na parte superior da tabela para filtrar a lista com base no status da conta-membro. Cada guia mostra o número de contas-membro correspondentes.

- Escolha Tudo para visualizar todas as contas-membro.
- Escolha Habilitado para visualizar contas com o status Habilitado.
- Escolha Não habilitado para visualizar contas com o status diferente de Habilitado.

Você também pode adicionar outros filtros à lista de contas-membro.

Para adicionar um filtro à lista de contas no gráfico de comportamento (console)

1. Escolha a caixa de filtro.
2. Escolha a coluna que você deseja usar para filtrar a lista.
3. Para a coluna especificada, escolha o valor a ser usado para o filtro.
4. Para remover um filtro, escolha o ícone x no canto superior direito.
5. Para atualizar a lista com as informações de status mais recentes, escolha o ícone de atualização no canto superior direito.

Listando suas contas de membros (Detective API,) AWS CLI

Você pode usar uma chamada de API ou a AWS Command Line Interface para ver uma lista de contas de membros em seu gráfico de comportamento.

Para obter o ARN do gráfico de comportamento para usar na solicitação, use a operação [ListGraphs](#).

Para recuperar uma lista de contas de membros (Detective API,) AWS CLI

- API do Detective: use a operação [ListMembers](#). Para identificar o gráfico de comportamento pretendido, especifique o ARN do gráfico de comportamento.

Observe que, para o gráfico de comportamento da organização, [ListMembers](#) não retorna as contas da organização que você não habilitou como contas-membro ou que você desassociou do gráfico de comportamento.

- AWS CLI: na linha de comando, execute o comando [list-members](#).

```
aws detective list-members --graph-arn <behavior graph ARN>
```

Exemplo:

```
aws detective list-members --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Para recuperar os detalhes de contas-membro específicas no gráfico de comportamento (API do Detective, AWS CLI)

- API do Detective: use a operação [GetMembers](#). Especifique o ARN do gráfico de comportamento e a lista de identificadores de conta das contas-membro.
- AWS CLI: na linha de comando, execute o comando [get-members](#).

```
aws detective get-members --account-ids <member account IDs> --graph-arn <behavior graph ARN>
```

Exemplo:

```
aws detective get-members --account-ids 444455556666 123456789012 --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Gerenciar contas da organização como contas-membro

No gráfico de comportamento da organização, a conta de administrador do Detective determina as contas da organização para serem habilitadas como contas-membro.

O Detective pode ser configurado para habilitar novas contas da organização como contas-membro automaticamente, ou as contas da organização podem ser habilitadas manualmente.

A conta de administrador do Detective também pode desassociar quaisquer contas da organização do gráfico de comportamento da organização.

Conteúdo

- [Habilitar novas contas da organização como contas-membro automaticamente](#)
- [Habilitar contas da organização como contas-membro](#)
- [Desassociar contas da organização como contas-membro](#)

Habilitar novas contas da organização como contas-membro automaticamente

A conta de administrador do Detective pode configurar o Detective para habilitar automaticamente novas contas da organização como contas-membro no gráfico de comportamento da organização.

Quando novas contas são adicionadas à organização, elas são adicionadas à lista na página Gerenciamento de contas. Para contas da organização, o Tipo é Por organização.

Por padrão, as novas contas da organização não são habilitadas como contas-membro. O status delas é Não é membro.

Ao escolher habilitar as contas da organização automaticamente, o Detective começa a habilitar novas contas como contas-membro à medida que forem adicionadas à organização. O Detective não habilita contas da organização que já existem e que ainda não estejam habilitadas.

Se o Detective pode ou não habilitar contas-membro da organização depende do seguinte:

- O número máximo de contas-membro em um gráfico de comportamento é 1.200. Se seu gráfico de comportamento já contiver 1.200 contas-membro, novas contas não poderão ser habilitadas.
- Detective não pode habilitar uma conta que não tenha a Amazon GuardDuty ativada por pelo menos 48 horas.
- O Detective não pode habilitar uma conta se isso fizer com que o volume de dados no gráfico de comportamento exceda o máximo permitido.

Habilitar novas contas da organização automaticamente (console)

Na página Gerenciamento de contas a configuração Habilitar automaticamente novas contas da organização determina a habilitação automática de novas contas à medida que são adicionadas a uma organização.

Para habilitar novas contas da organização como contas-membro automaticamente

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, escolha Gerenciamento de contas.
3. Ative Habilitar novas contas da organização automaticamente.

Ativando automaticamente novas contas da organização (Detective API,) AWS CLI

Para determinar se novas contas da organização podem ser habilitadas automaticamente, a conta de administrador pode usar a API do Detective ou a AWS Command Line Interface.

Para visualizar e gerenciar a configuração, você deve fornecer o ARN do gráfico de comportamento. Para obter o ARN, use a operação [ListGraphs](#).

Para visualizar a configuração atual para habilitar automaticamente as contas da organização

- API do Detective: use a operação [DescribeOrganizationConfiguration](#).

Na resposta, se as novas contas da organização forem habilitadas automaticamente, `AutoEnable` será `true`.

- AWS CLI: na linha de comando, execute o comando [describe-organization-configuration](#).

```
aws detective describe-organization-configuration --graph-arn <behavior graph ARN>
```

Exemplo

```
aws detective describe-organization-configuration --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Para habilitar novas contas da organização automaticamente

- API do Detective: use a operação [UpdateOrganizationConfiguration](#). Para habilitar novas contas da organização automaticamente, defina `AutoEnable` como `true`.
- AWS CLI: na linha de comando, execute o comando [update-organization-configuration](#).

```
aws detective update-organization-configuration --graph-arn <behavior graph ARN> --auto-enable | --no-auto-enable
```

Exemplo

```
aws detective update-organization-configuration --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234 --auto-enable
```

Habilitar contas da organização como contas-membro

Se você não habilitar automaticamente as novas contas da organização, poderá habilitar essas contas manualmente. Você também deve habilitar manualmente as contas que você desassociou.

Determinar se uma conta pode ser habilitada

Você não pode habilitar uma conta da organização como conta-membro se o gráfico de comportamento da organização já tiver o máximo de 1.200 contas habilitadas. Nesse caso, o status da conta da organização permanece Não é membro.

Quando você ativa a conta de uma organização, o Detective verifica se a conta é GuardDuty cliente da Amazon há pelo menos 48 horas. Em caso afirmativo, o Detective verifica se os dados da conta fariam com que a taxa de dados do gráfico de comportamento excedesse a cota. Essa verificação pode levar de 24 a 48 horas.

Enquanto o Detective verifica a taxa de dados, o status da conta-membro é Não habilitado.

Se a conta-membro passar pelas duas verificações, o status será atualizado para Habilitado. O Detective começa a ingestão de dados da conta-membro no gráfico de comportamento.

Se a conta falhar em uma dessas verificações, o status da conta-membro permanecerá Não habilitado. A conta não contribui com dados no gráfico de comportamento.

Assim que a conta-membro puder ser habilitada, o Detective altera automaticamente o status para Habilitado.

Habilitar contas da organização como contas-membro (console)

Na página Gerenciamento de contas, você pode habilitar as contas da organização como contas-membro.

Para habilitar contas da organização como contas-membro

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, escolha Gerenciamento de contas.
3. Para ver a lista de contas que não estão habilitadas no momento, escolha Não habilitado.
4. Você pode selecionar contas específicas da organização ou habilitar todas as contas da organização.

Para habilitar as contas da organização selecionadas:

- a. Selecione cada conta da organização que você deseja habilitar.
- b. Escolha Habilitar contas.

Para habilitar todas as contas da organização, escolha **Habilitar todas as contas da organização**.

Habilitando contas da organização como contas de membros (Detective API,) AWS CLI

Você pode usar a Detective API ou a AWS Command Line Interface para habilitar contas da organização como contas de membros no gráfico de comportamento da organização. Para obter o ARN do gráfico de comportamento para usar na solicitação, use a operação [ListGraphs](#).

Para habilitar contas da organização como contas de membros (Detective API,) AWS CLI

- API do Detective: use a operação [CreateMembers](#). Você deve fornecer o ARN do gráfico.

Para cada conta, especifique o identificador da conta. As contas da organização no gráfico de comportamento da organização não recebem um convite. Você não precisa fornecer um endereço de e-mail ou outras informações de convite.

- AWS CLI: na linha de comando, execute o comando [create-members](#).

```
aws detective create-members --accounts AccountId=<AWS account ID> --graph-arn <behavior graph ARN>
```

Exemplo

```
aws detective create-members --accounts AccountId=444455556666 AccountId=123456789012 --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Desassociar contas da organização como contas-membro

Para interromper a ingestão de dados de uma conta da organização no gráfico de comportamento da organização, você pode desassociar a conta. Os dados existentes dessa conta permanecem no gráfico de comportamento.

Ao desassociar uma conta da organização, o status muda para Não é membro. O Detective para a ingestão de dados dessa conta, mas a conta permanece na lista.

Desassociar contas da organização (console)

Na página Gerenciamento de contas, você pode desassociar as contas da organização como contas-membro.

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, escolha Gerenciamento de contas.
3. Para exibir a lista de contas habilitadas, escolha Habilitado.
4. Marque a caixa de seleção de cada conta a ser desassociada.
5. Escolha Ações. Em seguida, escolha Desabilitar contas.

O status das contas desassociadas muda para Não é membro.

Desassociando contas da organização (Detective API,) AWS CLI

Você pode usar a Detective API ou a AWS Command Line Interface para desassociar contas da organização como contas de membros em seu gráfico de comportamento.

Para obter o ARN do gráfico de comportamento para usar na solicitação, use a operação [ListGraphs](#).

Para desassociar contas da organização do gráfico de comportamento da organização (API do Detective, AWS CLI)

- API do Detective: use a operação [DeleteMembers](#). Especifique o ARN do gráfico e a lista de identificadores de conta das contas-membro a serem desassociadas.
- AWS CLI: na linha de comando, execute o comando [delete-members](#).

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior graph ARN>
```

Exemplo

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Gerenciar contas-membro convidadas

Uma conta de administrador também pode convidar contas para serem contas-membro em um gráfico de comportamento. Quando uma conta-membro aceita o convite e é habilitada, o Amazon Detective começa a ingestão e extração dos dados da conta-membro para esse gráfico de comportamento.

Para gráficos de comportamento que não sejam o da organização, todas as contas-membro são contas convidadas.

A conta de administrador do Detective também pode convidar contas que não sejam contas da organização para o gráfico de comportamento da organização.

A conta de administrador pode remover contas-membro convidadas do gráfico de comportamento.

Conteúdo

- [Convidar contas-membro para um gráfico de comportamento](#)
- [Habilitar uma conta-membro com status Não habilitado](#)
- [Remover contas-membro convidadas de um gráfico de comportamento](#)

Convidar contas-membro para um gráfico de comportamento

Uma conta de administrador pode convidar contas para contribuírem um gráfico de comportamento. Um gráfico de comportamento pode conter até 1.200 contas-membro.

Em um alto nível, o processo para convidar contas para contribuírem em um gráfico de comportamento é o seguinte.

1. Para cada conta de membro a ser adicionada, a conta de administrador fornece o identificador da AWS conta e o endereço de e-mail do usuário raiz.
2. O Detective valida se o endereço de e-mail é o endereço de e-mail do usuário raiz da conta.

Detective não realiza essa validação nas regiões (Leste dos EUA) ou AWS GovCloud AWS GovCloud (Oeste dos EUA).

3. Se as informações da conta forem válidas, o Detective envia o convite para a conta-membro.

Detective nunca envia convites por e-mail para contas de membros nas regiões (Leste dos EUA) ou AWS GovCloud AWS GovCloud (Oeste dos EUA).

Para outras regiões, a API do Detective inclui a opção de não enviar convites para as contas-membro.

Essa opção é útil para contas gerenciadas centralmente.

4. A conta-membro aceita ou recusa o convite.

Mesmo que a conta de administrador não envie e-mails de convite, a conta-membro ainda deverá responder ao convite.

5. Se a conta do membro aceitar o convite, o Detective verifica se a conta do membro é GuardDuty cliente da Amazon há pelo menos 48 horas.

Em caso afirmativo, o Detective verifica se os dados da conta-membro fariam com que a taxa de dados do gráfico de comportamento excedesse a cota.

Essa verificação pode levar entre 24 e 48 horas.

Enquanto o Detective verifica a taxa de dados, o status da conta-membro é Não habilitado.

6. Se a conta-membro passar pelas duas verificações, o status será automaticamente atualizado para Habilitado. O Detective começa a ingestão de dados da conta-membro no gráfico de comportamento.

Se a conta falhar em uma dessas verificações, o status da conta-membro permanecerá Não habilitado. A conta-membro não contribui com dados no gráfico de comportamento.

7. Assim que a conta-membro puder ser habilitada, o Detective altera automaticamente o status para Habilitado.

Por exemplo, o status da conta do membro muda para Ativada se a conta do membro for ativada GuardDuty e o Detective verificar se o volume de dados não é muito grande ou se a conta do administrador remover outras contas do membro para abrir espaço para uma conta.

Se mais de uma conta estiver Não habilitado, o Detective habilitará as contas na ordem em que foram convidadas. O processo para verificar se alguma conta com status Não habilitado será habilitada é feito a cada hora.

A conta de administrador também pode habilitar as contas manualmente, em vez de esperar pelo processo automático. Por exemplo, a conta de administrador pode selecionar as contas a serem habilitadas. Consulte [the section called “Habilitar uma conta-membro com status Não habilitado”](#).

Observe que o Detective começou a habilitar automaticamente contas com o status Não habilitado em 12 de maio de 2021. As contas com status Não habilitado antes dessa data não são habilitadas automaticamente. A conta de administrador deve habilitá-las manualmente.

Convidar contas individuais para um gráfico de comportamento (Console)

Você pode especificar manualmente as contas-membro a serem convidadas para contribuírem com seus dados para um gráfico de comportamento.

Para selecionar manualmente as contas-membro a serem convidadas (console)

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, escolha Gerenciamento de contas.
3. Escolha Ações. Em seguida, escolha Convidar contas.
4. Em Adicionar contas, escolha Adicionar contas individuais.
5. Para adicionar uma conta-membro à lista de convites, execute as etapas a seguir.
 - a. Escolha Adicionar conta.
 - b. Em ID AWS da conta, insira a ID da AWS conta.
 - c. Em Endereço de e-mail, insira o endereço de e-mail da conta do usuário raiz.
6. Para remover uma conta da lista, escolha Remover essa conta.
7. Em Personalizar e-mail de convite, adicione conteúdo personalizado para incluir no e-mail de convite.

Por exemplo, você pode usar essa área para fornecer informações de contato. Ou use-o para lembrar à conta-membro de que é necessário anexar a política do IAM necessária ao usuário ou à função antes de aceitar o convite.

8. A política do IAM da conta-membro contém o texto da política do IAM necessária para as contas-membro. O convite por e-mail inclui esse texto da política. Para copiar o texto da política, escolha Copiar.
9. Escolha Convidar.

Convidar uma lista de contas-membro para um gráfico de comportamento (Console)

No console do Detective, você pode fornecer um arquivo `.csv` contendo uma lista de contas-membro a serem convidadas para seu gráfico de comportamento.

A primeira linha do arquivo é a linha de cabeçalho. Cada conta é listada em uma linha separada. Cada entrada da conta do membro contém o ID da AWS conta e o endereço de e-mail do usuário raiz da conta.

Exemplo:

```
Account ID,Email address
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

Quando o Detective processa o arquivo, ele ignora as contas que já foram convidadas, a menos que o status da conta seja Verificação falhou. Esse status indica que o endereço de e-mail fornecido para a conta não corresponde ao endereço de e-mail do usuário raiz da conta. Nesse caso, o Detective exclui o convite original e tenta verificar o endereço de e-mail e enviar o convite outra vez.

Essa opção também fornece um modelo que pode ser usado para criar a lista de contas.

Para convidar contas-membro de uma lista em `.csv` (console)

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, escolha Gerenciamento de contas.
3. Escolha Ações. Em seguida, escolha Convidar contas.
4. Em Adicionar contas, escolha Adicionar de um `.csv`.
5. Para baixar um arquivo de modelo para trabalhar, escolha Baixar modelo em `.csv`.
6. Para selecionar o arquivo contendo a lista de contas, escolha Escolher arquivo em `.csv`.
7. Em Revisar contas-membro, verifique a lista de contas-membro que o Detective encontrou no arquivo.
8. Em Personalizar e-mail de convite, adicione conteúdo personalizado para incluir no e-mail de convite.

Por exemplo, você pode fornecer informações de contato ou lembrar à conta-membro sobre a política do IAM necessária.

9. A política do IAM da conta-membro contém o texto da política do IAM necessária para as contas-membro. O convite por e-mail inclui esse texto da política. Para copiar o texto da política, escolha Copiar.
10. Escolha Convidar.

Convidar contas de membros para um gráfico de comportamento (Detective API,) AWS CLI

Você pode usar a Detective API ou a AWS Command Line Interface para convidar contas de membros a contribuir com seus dados para um gráfico de comportamento. Para obter o ARN do gráfico de comportamento para usar na solicitação, use a operação [ListGraphs](#).

Para convidar contas de membros para um gráfico de comportamento (Detective API,) AWS CLI

- API do Detective: use a operação [CreateMembers](#). Você deve fornecer o ARN do gráfico. Para cada conta, especifique o identificador da conta e o endereço de e-mail do usuário raiz.

Para não enviar e-mails de convite para as contas-membro, defina `DisableEmailNotification` como verdadeiro. Por padrão, `DisableEmailNotification` é falso.

Se você enviar e-mails de convite, você pode optar por adicionar texto personalizado ao e-mail de convite.

- AWS CLI: na linha de comando, execute o comando `create-members`.

```
aws detective create-members --accounts AccountId=<AWS account ID>,EmailAddress=<root user email address> --graph-arn <behavior graph ARN> --message "<Custom message text>"
```

Exemplo

```
aws detective create-members --accounts
AccountId=444455556666,EmailAddress=mmajor@example.com
AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
arn:aws:detective:us-east-1:111122223333:graph:123412341234 --message "This is Paul
Santos. I need to add your account to the data we use for security investigation in
Amazon Detective. If you have any questions, contact me at psantos@example.com."
```

Para indicar que e-mails de convite não devem ser enviados a contas-membro, inclua `--disable-email-notification`.

```
aws detective create-members --accounts AccountId=<AWS account ID>,EmailAddress=<root user email address> --graph-arn <behavior graph ARN> --disable-email-notification
```

Exemplo

```
aws detective create-members --accounts
  AccountId=444455556666,EmailAddress=mmajor@example.com
  AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
  arn:aws:detective:us-east-1:111122223333:graph:123412341234 --disable-email-
  notification
```

Adicionar uma lista de contas de membros em todas as regiões (script Python ativado) GitHub

Detective fornece um script de código aberto GitHub que permite que você faça o seguinte:

- Adicionar uma lista específica de contas-membro aos gráficos de comportamento de uma conta de administrador em uma lista específica de regiões.
- Se a conta de administrador não tiver um gráfico de comportamento em uma região, o script também habilitará o Detective e criará o gráfico de comportamento nessa região.
- Enviar e-mails de convite para as contas-membro.
- Aceitar automaticamente os convites para as contas-membro.

Para obter informações sobre como configurar e usar os GitHub scripts, consulte [the section called “Scripts em Python do Amazon Detective”](#).

Habilitar uma conta-membro com status Não habilitado

Depois que uma conta-membro aceita um convite, o Amazon Detective verifica se pode habilitar a conta-membro. Se o Detective não conseguir habilitar a conta-membro, ele definirá o status da conta-membro como Não habilitado. Isso pode acontecer por um dos seguintes motivos.

- A conta do membro não é GuardDuty cliente da Amazon há pelo menos 48 horas.

- O Detective está verificando o volume de dados da conta-membro.
- Os dados da conta-membro fariam com que o volume de dados do gráfico de comportamento excedesse a cota.

As contas-membro com status Não habilitado não contribuem com dados para o gráfico de comportamento.

O Detective habilita as contas automaticamente, pois o gráfico de comportamento pode acomodá-las.

Você também pode tentar habilitar manualmente contas-membro com status Não habilitado. Por exemplo, você pode remover contas-membro existentes para reduzir o volume de dados. Em vez de esperar pelo processo automático para habilitar contas, você pode tentar habilitar contas-membro com status Não habilitado.

Habilitar uma conta-membro com status Não habilitado (Console)

A lista de contas-membro inclui uma opção para habilitar contas-membro selecionadas com status Não habilitado.

Para habilitar uma conta-membro com status Não habilitado

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, escolha Gerenciamento de contas.
3. Em Minhas contas-membro, marque a caixa de seleção de cada conta-membro a ser habilitada.

Você só pode habilitar contas-membro com o status Não habilitado.

4. Escolha Habilitar contas.

O Detective determina se a conta-membro pode ser habilitada. Se a conta-membro puder ser habilitada, o status mudará para Habilitado.

Ativando uma conta de membro que não está ativada (Detective API,) AWS CLI

Você pode usar uma chamada de API ou a AWS Command Line Interface para habilitar uma conta de membro único que não esteja ativada. Para obter o ARN do gráfico de comportamento para usar na solicitação, use a operação [ListGraphs](#).

Para habilitar uma conta-membro com status Não habilitado

- API do Detective: use a operação [StartMonitoringMember](#) da API. Você deve fornecer o ARN do gráfico de comportamento. Para identificar a conta do membro, use o identificador da AWS conta.
- AWS CLI: na linha de comando, execute o comando [start-monitoring-member](#):

```
start-monitoring-member --graph-arn <behavior graph ARN> --account-id <AWS account ID>
```

Por exemplo: .

```
start-monitoring-member --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234 --account-id 444455556666
```

Remover contas-membro convidadas de um gráfico de comportamento

A conta de administrador pode remover contas-membro de um gráfico de comportamento a qualquer momento.

Detective remove automaticamente as contas dos membros que estão encerradas AWS, exceto nas regiões (Leste dos EUA) e AWS GovCloud AWS GovCloud (Oeste dos EUA).

Quando uma conta-membro convidada é removida de um gráfico de comportamento, ocorre o seguinte.

- A conta-membro é removida de Minhas contas-membro.
- O Amazon Detective para a ingestão de dados da conta removida.

O Detective não remove nenhum dado existente do gráfico de comportamento, que agrega dados das contas-membro.

Remover contas-membro convidadas de um gráfico de comportamento (console)

Você pode usar o AWS Management Console para remover contas de membros convidados do seu gráfico de comportamento.

Para remover contas-membro (console)

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, escolha Gerenciamento de contas.
3. Na lista de contas, marque a caixa de seleção de cada conta-membro a ser removida.

Você não pode remover sua própria conta da lista.

4. Escolha Ações. Em seguida, escolha Desabilitar contas.

Removendo contas de membros convidados de um gráfico de comportamento (Detective API,) AWS CLI

Você pode usar a Detective API ou a AWS Command Line Interface para remover contas de membros convidados do seu gráfico de comportamento. Para obter o ARN do gráfico de comportamento para usar na solicitação, use a operação [ListGraphs](#).

Para remover contas de membros convidados do seu gráfico de comportamento (Detective API,) AWS CLI

- API do Detective: use a operação [DeleteMembers](#). Especifique o ARN do gráfico e a lista de identificadores de conta das contas-membro a serem removidas.
- AWS CLI: na linha de comando, execute o comando [delete-members](#).

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior graph ARN>
```

Exemplo:

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Removendo uma lista de contas de membros convidados em todas as regiões (script Python ativado) GitHub

Detective fornece um script de código aberto em [GitHub](#). Esse script pode ser usado para remover uma lista específica de contas-membro dos gráficos de comportamento de uma conta de administrador em uma lista específica de regiões.

Para obter informações sobre como configurar e usar os GitHub scripts, consulte [the section called “Scripts em Python do Amazon Detective”](#).

Para contas-membro: gerenciar convites e associações a gráficos de comportamento

O Amazon Detective cobra de cada conta-membro pela ingestão de dados em cada gráfico de comportamento ao qual contribui.

A página Gerenciamento de contas permite que as contas-membro vejam as contas de administrador dos gráficos de comportamento dos quais são membros.

As contas-membro que são convidadas para um gráfico de comportamento podem visualizar e responder aos convites. Também podem remover sua própria conta do gráfico de comportamento.

Para o gráfico de comportamento da organização, as contas da organização não controlam se a própria conta é uma conta-membro. A conta de administrador do Detective escolhe as contas da organização para serem habilitadas ou desabilitadas como contas-membro.

Conteúdo

- [Política do IAM necessária para uma conta-membro](#)
- [Visualizar sua lista de convites para gráficos de comportamento](#)
- [Responder a um convite para um gráfico de comportamento](#)
- [Remover sua conta de um gráfico de comportamento](#)

Política do IAM necessária para uma conta-membro

Antes que uma conta-membro possa visualizar e gerenciar convites, a política do IAM necessária deve ser anexada à entidade principal. A entidade principal pode ser um usuário ou uma função existente, ou você pode criar um novo usuário ou função para usar no Detective.

O ideal é que a conta de administrador faça com que o administrador do IAM anexe a política necessária.

A política do IAM da conta-membro concede acesso às ações da conta-membro no Amazon Detective. O convite por e-mail para contribuir em um gráfico de comportamento inclui o texto dessa política do IAM.

Para usar essa política, substitua *<behavior graph ARN>* pelo ARN do gráfico.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:DisassociateMembership",
        "detective:RejectInvitation"
      ],
      "Resource": "<behavior graph ARN>"
    },
    {
      "Effect": "Allow",
      "Action": [
        "detective:BatchGetMembershipDatasources",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations"
      ],
      "Resource": "*"
    }
  ]
}
```

Observe que as contas da organização no gráfico de comportamento da organização não recebem convites e não podem desassociar suas contas do gráfico de comportamento da organização. Se não pertencerem a outros gráficos de comportamento, precisarão somente da permissão `ListInvitations`. `ListInvitations` permite que essas contas vejam a conta de administrador do gráfico de comportamento. As permissões para gerenciar convites e desassociar associações se aplicam somente às associações por convite.

Visualizar sua lista de convites para gráficos de comportamento

No console do Amazon Detective, na API Detective ou AWS Command Line Interface na conta de um membro pode ver seus convites do gráfico de comportamento.

Visualizar convites para gráficos de comportamento (console)

Você pode ver os convites do gráfico de comportamento no AWS Management Console

Para visualizar convites para gráficos de comportamento (console)

1. Faça login no AWS Management Console. Em seguida, abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, escolha Gerenciamento de contas.

Na página Gerenciamento de contas, Minhas contas de administrador contém seus convites para gráficos de comportamento abertos e aceitos na região atual. Para uma conta da organização, Minhas contas de administrador também contém o gráfico de comportamento da organização.

Se sua conta estiver atualmente no período de teste gratuito, a página também exibirá o número de dias restantes em seu teste gratuito.

A lista não contém convites que você recusou, associações às quais você renunciou ou associações que a conta de administrador removeu.

Cada convite mostra o número da conta de administrador, a data em que o convite foi aceito e o status atual do convite.

- Para convites aos quais você não respondeu, o status é Convidado.
- Para convites que você aceitou, o status é Habilitado ou Não habilitado.

Se o status for Habilitado, sua conta contribuirá com dados no gráfico de comportamento.

Se o status for Não habilitado, sua conta não contribuirá com dados no gráfico de comportamento.

O status da sua conta é definido inicialmente como Não ativada, enquanto o Detective verifica se você GuardDuty ativou e, em caso afirmativo, se sua conta faria com que o volume de dados do gráfico de comportamento excedesse a cota de Detective.

Se sua conta não fizer com que o gráfico de comportamento exceda a cota, o Detective atualizará o status da sua conta para Habilitado. Caso contrário, o status permanecerá Não habilitado.

Quando o gráfico de comportamento consegue acomodar o volume de dados da sua conta, o Detective o atualiza automaticamente para Habilitado. Por exemplo, a conta de administrador pode

remover outras contas-membro para que sua conta possa ser habilitada. A conta de administrador também pode habilitar sua conta manualmente.

Visualizar convites para gráficos de comportamento (API do Detective, AWS CLI)

Você pode listar os convites para gráficos de comportamento na API do Detective ou no AWS Command Line Interface.

Para recuperar uma lista de convites para gráficos de comportamento abertos e aceitos (API do Detective, AWS CLI)

- API do Detective: use a operação [ListInvitations](#).
- AWS CLI: na linha de comando, execute o comando [list-invitations](#).

```
aws detective list-invitations
```

Responder a um convite para um gráfico de comportamento

Ao aceitar um convite, o status da sua conta é definido inicialmente como Não habilitado enquanto o Detective verifica se sua conta faria com que o volume de dados do gráfico de comportamento excedesse a cota do Detective. Para que o Detective faça essa verificação, sua conta deve ter a Amazon GuardDuty ativada por pelo menos 48 horas.

Se sua conta não fizer com que o gráfico de comportamento exceda a cota, o Detective atualizará o status da sua conta para Habilitado. O Detective começa a ingestão e extração de dados de logs e descobertas no gráfico de comportamento a partir desse momento. A conta é cobrada pelos dados.

Se a adição de sua conta fizer com que o volume de dados do gráfico de comportamento exceda a cota de Detective, ou se você não tiver GuardDuty ativado, o status permanecerá Não ativado. Nesse caso, a menos que você remova sua conta, o Detective habilita automaticamente sua conta assim que o gráfico de comportamento puder acomodá-la. A conta de administrador também pode habilitar sua conta manualmente.

Se você recusar o convite, ele será removido da sua lista de convites e o Detective não usará os dados da sua conta no gráfico de comportamento.

Responder a um convite para um gráfico de comportamento (console)

Você pode usar o AWS Management Console para responder ao convite por e-mail, que inclui um link para o console do Detective. Você só pode responder a um convite com o status Convidado.

Para responder a um convite para um gráfico de comportamento (console)

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, escolha Gerenciamento de contas.
3. Em Minhas contas de administrador, para aceitar o convite e começar a contribuir com dados no gráfico de comportamento, escolha Aceitar convite.

Para recusar o convite e removê-lo da lista, escolha Recusar.

Respondendo a um convite de gráfico de comportamento (Detective API,) AWS CLI

Você pode responder a convites para gráficos de comportamento na API do Detective ou no AWS Command Line Interface.

Para aceitar um convite de gráfico de comportamento (Detective API,) AWS CLI

- API do Detective: use a operação [AcceptInvitation](#). Você deve especificar o ARN do gráfico.
- AWS CLI: na linha de comando, execute o comando [accept-invitation](#).

```
aws detective accept-invitation --graph-arn <behavior graph ARN>
```

Exemplo:

```
aws detective accept-invitation --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Para recusar um convite para um gráfico de comportamento (Detective API,) AWS CLI

- API do Detective: use a operação [RejectInvitation](#). Você deve especificar o ARN do gráfico.
- AWS CLI: na linha de comando, execute o comando [reject-invitation](#).

```
aws detective reject-invitation --graph-arn <behavior graph ARN>
```

Exemplo:

```
aws detective reject-invitation --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Remover sua conta de um gráfico de comportamento

Depois de aceitar um convite, você pode remover sua conta de um gráfico de comportamento a qualquer momento. Ao remover sua conta de um gráfico de comportamento, o Amazon Detective para a ingestão de dados da sua conta no gráfico de comportamento. Os dados existentes permanecem no gráfico de comportamento.

Somente contas convidadas podem remover suas contas de um gráfico de comportamento. As contas da organização não podem se remover do gráfico de comportamento da organização.

Remover sua conta de um gráfico de comportamento (Console)

Você pode usar o AWS Management Console para remover sua conta de um gráfico de comportamento.

Para remover sua conta de um gráfico de comportamento (console)

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, escolha Gerenciamento de contas.
3. Em Minhas contas de administrador, para o gráfico de comportamento do qual você deseja renunciar, escolha Renunciar.

Removendo sua conta de um gráfico de comportamento (Detective API,) AWS CLI

Você pode usar a Detective API ou a AWS Command Line Interface para remover sua conta de um gráfico de comportamento.

Para remover sua conta de um gráfico de comportamento (Detective API,) AWS CLI

- API do Detective: use a operação [DisassociateMembership](#). Você deve especificar o ARN do gráfico.
- AWS CLI: na linha de comando, execute o comando [disassociate-membership](#).


```
aws detective disassociate-membership --graph-arn <behavior graph ARN>
```

Exemplo:

```
aws detective disassociate-membership --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Efeito das ações da conta nos gráficos de comportamento

Essas ações têm os seguintes efeitos nos dados e no acesso do Amazon Detective.

Detective desabilitado

Quando uma conta de administrador desabilita o Detective, ocorre o seguinte:

- O gráfico de comportamento é removido.
- O Detective para a ingestão de dados da conta de administrador e das contas-membro para esse gráfico de comportamento.

Conta-membro removida do gráfico de comportamento

Quando uma conta-membro é removida de um gráfico de comportamento, o Detective para a ingestão de dados dessa conta.

Os dados existentes no gráfico de comportamento não são afetados.

Para contas convidadas, a conta é removida da lista Minhas contas-membro.

Para contas da organização no gráfico de comportamento da organização, o status da conta muda para Não é membro.

A conta-membro sai da organização

Quando uma conta-membro sai de uma organização, ocorre o seguinte:

- A conta é removida da lista Minhas contas-membro do gráfico de comportamento da organização.

- O Detective para a ingestão de dados dessa conta.

Os dados existentes no gráfico de comportamento não são afetados.

AWS conta suspensa

Quando uma conta de administrador é suspensa AWS, a conta perde a permissão para visualizar o gráfico de comportamento em Detective. O Detective para a ingestão de dados no gráfico de comportamento.

Quando a conta de um membro é suspensa AWS, o Detective para de ingerir dados dessa conta.

Após 90 dias, a conta é encerrada ou reabilitada. Quando uma conta de administrador é reabilitada, suas permissões do Detective são restauradas. O Detective retoma a ingestão de dados da conta. Quando uma conta-membro é reabilitada, o Detective retoma a ingestão de dados da conta.

AWS conta fechada

Quando uma AWS conta é fechada, o Detective responde ao encerramento da seguinte forma.

- Para uma conta de administrador, o Detective exclui o gráfico de comportamento.
- Para uma conta-membro, o Detective remove a conta do gráfico de comportamento.

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

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

Important

Para clientes nas AWS GovCloud (US) regiões:

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

Usando os scripts do Amazon Detective Python para gerenciar contas

O Amazon Detective fornece um conjunto de scripts Python de código aberto no repositório. [GitHub amazon-detective-multiaccount-scripts](#) Os scripts exigem o Python 3.

É possível usá-los para realizar as seguintes tarefas:

- Habilitar o Detective para uma conta de administrador entre regiões.

Ao habilitar o Detective, você pode atribuir valores de tag ao gráfico de comportamento.

- Adicionar contas-membro aos gráficos de comportamento de uma conta de administrador entre regiões.
- Optar por enviar e-mails de convite para as contas-membro. Você também pode configurar a solicitação para não enviar e-mails de convite.
- Remover contas-membro dos gráficos de comportamento de uma conta de administrador entre regiões.
- Desabilitar o Detective para uma conta de administrador entre regiões. Quando uma conta de administrador desabilita o Detective, o gráfico de comportamento da conta de administrador em cada região é desabilitado.

Visão geral do script **enableDetective.py**

O script `enableDetective.py` faz o seguinte:

1. Habilita a entrada do Detective em uma conta de administrador em cada região especificada, se a conta de administrador ainda não tiver o Detective habilitado nessa região.

Ao usar o script para habilitar o Detective, você pode atribuir valores de tag ao gráfico de comportamento.

2. Opta por enviar convites da conta de administrador para as contas-membro especificadas para cada gráfico de comportamento.

As mensagens de e-mail dos convites usam o conteúdo padrão da mensagem e não podem ser personalizadas.

Você também pode configurar a solicitação para não enviar e-mails de convite.

3. Aceita automaticamente os convites para as contas-membro.

Como o script aceita automaticamente os convites, as contas-membro podem ignorar essas mensagens.

Recomendamos entrar em contato diretamente com as contas-membro para notificá-las de que os convites são aceitos automaticamente.

Visão geral do script **disableDetective.py**

O script `disableDetective.py` exclui as contas-membro especificadas dos gráficos de comportamento da conta de administrador nas regiões especificadas.

Também oferece a opção de desabilitar o Detective da conta de administrador nas regiões especificadas.

Permissões necessárias para os scripts

Os scripts exigem uma AWS função preexistente na conta do administrador e em todas as contas de membros que você adiciona ou remove.

Note

O nome da função deve ser o mesmo em todas as contas.

A política do IAM [melhores práticas recomendadas](#) são para usar funções de menor escopo. Para executar o fluxo de trabalho do script de [criar um gráfico](#), [criar membros](#) e [adicionar membros ao gráfico](#), as permissões necessárias são:

- `detetive: CreateGraph`
- `detetive: CreateMembers`
- `detetive: DeleteGraph`
- `detetive: DeleteMembers`

- `detetive: ListGraphs`
- `detetive: ListMembers`
- `detetive: AcceptInvitation`

Relação de confiança da função

A relação de confiança da função deve permitir que sua instância ou suas credenciais locais assumam a função.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<ACCOUNTID>:user/<USERNAME>"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Se você não tiver uma função comum que inclua as permissões necessárias, deverá criar uma função com pelo menos essas permissões em cada conta-membro. Você também deve criar a função na conta de administrador.

Ao criar a função, certifique-se de fazer o seguinte:

- Use o mesmo nome de função em todas as contas.
- Adicione as permissões necessárias acima (recomendado) ou selecione a política [AmazonDetectiveFullAccess](#) gerenciada.
- Adicione um bloco de relação de confiança da função, conforme discutido acima.

Para automatizar esse processo, você pode usar o `EnableDetective.yaml` AWS CloudFormation modelo. Como o modelo cria somente recursos globais, ele pode ser executado em qualquer região.

Configurar o ambiente de execução dos scripts do Python

Você pode executar os scripts de uma instância do EC2 ou de uma máquina local.

Iniciar e configurar uma instância do EC2

Uma opção para executar os scripts é executá-los a partir de uma instância do EC2.

Para iniciar e configurar uma instância do EC2

1. Inicie uma instância do EC2 na sua conta de administrador. Para obter mais informações sobre como iniciar uma instância do EC2, consulte [Conceitos básicos de instâncias Linux do Amazon EC2](#) no Guia do usuário do Amazon EC2 para instâncias Linux.
2. Anexe à instância um perfil do IAM que tenha permissões para permitir que a instância acione AssumeRole dentro da conta de administrador.

Se você usou o EnableDetective.yaml AWS CloudFormation modelo, uma função de instância com um perfil chamado EnableDetective foi criada.

Caso contrário, para obter informações sobre como criar uma função de instância, consulte a postagem do blog [Substituir ou anexar facilmente um perfil do IAM a uma instância do EC2 existente usando o console do EC2](#).

3. Instalar o software necessário:
 - APT: `sudo apt-get -y install python3-pip python3 git`
 - RPM: `sudo yum -y install python3-pip python3 git`
 - Boto (versão mínima 1.15): `sudo pip install boto3`
4. Clone o repositório na instância do EC2.

```
git clone https://github.com/aws-samples/amazon-detective-multiaccount-scripts.git
```

Configurar uma máquina local para executar os scripts

Você também pode executar os scripts a partir da máquina local.

Para configurar uma máquina local para executar os scripts

1. Certifique-se de ter configurado em sua máquina local as credenciais da sua conta de administrador que tenha permissão para acionar AssumeRole.
2. Instale o software necessário:
 - Python 3

- Boto (versão mínima 1.15)
- GitHub scripts

Plataforma	Instruções de configuração
Windows	<ol style="list-style-type: none">1. Instale o Python 3 (https://www.python.org/downloads/windows/).2. Abra um prompt de comando.3. Para instalar o Boto, execute: <code>pip install boto3</code>4. Baixe o código-fonte do script em GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts).
Mac	<ol style="list-style-type: none">1. Instale o Python 3 (https://www.python.org/downloads/mac-osx/).2. Abra um prompt de comando.3. Para instalar o Boto, execute: <code>pip install boto3</code>4. Baixe o código-fonte do script em GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts).
Linux	<ol style="list-style-type: none">1. Para instalar o Python 3, execute uma das seguintes opções:<ul style="list-style-type: none">• <code>sudo apt-get -y install python3-pip python3 git</code>• <code>sudo yum install git python</code>2. Para instalar o Boto, execute: <code>sudo pip install boto3</code>3. Clone o código-fonte do script em https://github.com/aws-samples/amazon-detective-multiaccount-scripts.

Criar uma lista em `.csv` de contas-membro a adicionar ou remover

Para identificar as contas-membro a serem adicionadas ou removidas dos gráficos de comportamento, forneça um arquivo `.csv` contendo a lista de contas.

Liste cada conta em uma linha separada. Cada entrada da conta do membro contém o ID da AWS conta e o endereço de e-mail do usuário raiz da conta.

Veja o exemplo a seguir:

```
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

Executar o `enableDetective.py`

Você pode executar o script `enableDetective.py` de uma instância do EC2 ou de uma máquina local.

Para executar o `enableDetective.py`

1. Copie o arquivo `.csv` para o diretório `amazon-detective-multiaccount-scripts` em sua instância do EC2 ou máquina local.
2. Mude para o diretório `amazon-detective-multiaccount-scripts`.
3. Execute o script `enableDetective.py`.

```
enableDetective.py --master_account administratorAccountID --assume_role roleName
--input_file inputFileName --tags tagValueList --enabled_regions regionList --
disable_email
```

Ao executar o script, substitua os seguintes valores:

administratorAccountID

O AWS ID da conta do administrador.

roleName

O nome da AWS função a ser assumida na conta do administrador e na conta de cada membro.

inputFileName

O nome do arquivo .csv contendo a lista de contas-membro a serem adicionadas aos gráficos de comportamento da conta de administrador.

tagValueList

(Opcional) Uma lista separada por vírgulas de valores de tags para atribuir a um novo gráfico de comportamento.

Para cada valor de tag, o formato é *key=value*. Por exemplo: .

```
--tags Department=Finance,Geo=Americas
```

regionList

(Opcional) Uma lista separada por vírgulas das regiões nas quais adicionar as contas-membro ao gráfico de comportamento da conta de administrador. Por exemplo: .

```
--enabled_regions us-east-1,us-east-2,us-west-2
```

Talvez a conta de administrador ainda não tenha o Detective habilitado em uma região. Nesse caso, o script habilita o Detective e cria um novo gráfico de comportamento para a conta de administrador.

Se você não fornecer uma lista de regiões, o script atuará em todas as regiões compatíveis com o Detective.

`--disable_email`

(Opcional) Se incluído, o Detective não envia e-mails de convite para as contas-membro.

Executar o **disableDetective.py**

Você pode executar o script `disableDetective.py` de uma instância do EC2 ou de uma máquina local.

Para executar o **disableDetective.py**

1. Copie os arquivos .csv no diretório `amazon-detective-multiaccount-scripts`.

2. Para usar o arquivo `.csv` para excluir as contas-membro listadas dos gráficos de comportamento da conta de administrador em uma lista específica de regiões, execute o script `disableDetective.py` da seguinte forma:

```
disabledetective.py --master_account administratorAccountID --assume_role roleName  
--input_file inputFileName --disabled_regions regionList
```

3. Para desabilitar o Detective na conta de administrador em todas as regiões, execute o script `disableDetective.py` com o sinalizador `--delete-master`.

```
disabledetective.py --master_account administratorAccountID --assume_role roleName  
--input_file inputFileName --disabled_regions regionList --delete_master
```

Ao executar o script, substitua os seguintes valores:

administratorAccountID

O AWS ID da conta do administrador.

roleName

O nome da AWS função a ser assumida na conta do administrador e na conta de cada membro.

inputFileName

O nome do arquivo `.csv` contendo a lista de contas-membro a serem removidas dos gráficos de comportamento da conta de administrador.

Você deve fornecer um arquivo `.csv` mesmo se estiver desabilitando o Detective.

regionList

(Opcional) Uma lista separada por vírgulas de regiões nas quais realizar uma das seguintes ações:

- Remover as contas-membro dos gráficos de comportamento da conta de administrador.
- Se o sinalizador `--delete-master` estiver incluído, desabilite o Detective.

Por exemplo: .

```
--disabled_regions us-east-1,us-east-2,us-west-2
```

Se você não fornecer uma lista de regiões, o script atuará em todas as regiões compatíveis com o Detective.

Integração com o Amazon Security Lake

O Amazon Security Lake é um serviço de data lake de segurança totalmente gerenciado. Você pode usar o Security Lake para centralizar automaticamente os dados de segurança de AWS ambientes, provedores de SaaS, fontes locais, fontes de nuvem e fontes de terceiros em um data lake específico que é armazenado em sua conta. O Amazon Security Lake ajuda você a analisar dados de segurança, para que você tenha uma compreensão mais integral das posturas de segurança de toda a organização. Com o Security Lake, você também pode melhorar a proteção das suas workloads, aplicações e dados.

O Amazon Detective se integra ao Amazon Security Lake, o que significa que você pode consultar e recuperar os dados de log bruto armazenados pelo Security Lake.

Usando essa integração, você pode coletar logs e eventos das fontes a seguir, às quais o Security Lake oferece suporte nativo. O Detective suporta até a versão de origem 2 (OCSF 1.1.0).

- AWS CloudTrail eventos de gerenciamento versão 1.0 e posteriores
- Logs de fluxo da Amazon Virtual Private Cloud (Amazon VPC) versão 1.0 e posterior
- Log de auditoria do Amazon Elastic Kubernetes Service (Amazon EKS) versão 2.0. Para usar os registros de auditoria do Amazon EKS como fonte, você deve adicionar permissões `iam:ListResources` ao IAM. Para obter mais detalhes, consulte [Adicionar as permissões necessárias do IAM à sua conta](#).

[Para obter detalhes sobre como o Security Lake converte automaticamente registros e eventos provenientes de AWS serviços com suporte nativo no esquema OCSF, consulte o Guia do usuário do Amazon Security Lake.](#)

Depois de integrar o Detective ao Security Lake, o Detective começa a extrair registros brutos do Security Lake relacionados a eventos de gerenciamento AWS CloudTrail e aos registros de fluxo do Amazon VPC. Para obter mais detalhes, consulte [Querying raw logs](#).

Para integrar o Detective ao Security Lake, conclua as seguintes etapas:

1. [Antes de começar](#)

Use uma conta de gerenciamento do Organizations para designar um administrador delegado do Security Lake para a organização. Certifique-se de que o Security Lake esteja ativado e

verifique se o Security Lake está coletando registros e eventos de eventos de AWS CloudTrail gerenciamento e registros de fluxo da Amazon Virtual Private Cloud (Amazon VPC).

Em alinhamento com a Arquitetura de Referência de Segurança, o Detective recomenda usar uma conta do Log Archive e deixar de usar uma conta do Security Tooling para a implantação do Security Lake.

2. [Criar um assinante do Security Lake](#)

Você deve ser um assinante do Amazon Security Lake para consumir logs e eventos do Security Lake. Siga estas etapas para conceder acesso de consulta a um administrador de conta do Detective.

3. Adicione as permissões necessárias AWS Identity and Access Management (IAM) à sua identidade do IAM.

- Adicione essas permissões para criar a integração do Detective com o Security Lake:
 - Anexe essas permissões de AWS Identity and Access Management (IAM) à sua identidade do IAM. Para obter detalhes, consulte a seção [Adicionar as permissões necessárias do IAM à sua conta](#).
 - Adicione essa política do IAM ao principal do IAM que você planeja usar para transmitir a função AWS CloudFormation de serviço. Para obter mais detalhes, consulte a seção [Adicionar permissões ao seu IAM principal](#).
 - Se você já integrou o Detective ao Security Lake, para usar a integração, anexe essas permissões (IAM) à sua identidade do IAM. Para obter detalhes, consulte a seção [Adicionar as permissões necessárias do IAM à sua conta](#).

4. [Aceitar o convite do ARN do compartilhamento de recursos e habilitar a integração](#)

Use o AWS CloudFormation modelo para configurar os parâmetros necessários para criar e gerenciar o acesso a consultas para assinantes do Security Lake. Para ver as etapas detalhadas para criar uma pilha, consulte [Criar uma pilha usando o AWS CloudFormation modelo](#). Depois de criar a pilha, habilite a integração.

Para uma demonstração de como integrar o Amazon Detective com o Amazon Security Lake usando o console Detective, assista ao seguinte vídeo: [Integração do Amazon Detective com o Amazon Security Lake- Como configurar -->](#)

Antes de começar

O Security Lake se integra AWS Organizations para gerenciar a coleta de registros em várias contas em uma organização. Para usar o Security Lake em uma organização, sua conta AWS Organizations de gerenciamento deve primeiro designar um administrador delegado do Security Lake para sua organização. O administrador delegado do Security Lake deve então habilitar o Security Lake e habilitar a coleta de logs e eventos para contas-membro na organização.

Antes de integrar o Security Lake ao Detective, garanta que o Security Lake está habilitado para a conta de administrador do Security Lake. Para obter as etapas detalhadas sobre como habilitar o Security Lake, consulte [Conceitos básicos](#) no Guia do usuário do Amazon Security Lake.

Além disso, verifique se o Security Lake está coletando registros e eventos de eventos de AWS CloudTrail gerenciamento e registros de fluxo da Amazon Virtual Private Cloud (Amazon VPC). Para obter mais detalhes sobre a coleta de registros no Security Lake, consulte [Coleta de dados de AWS serviços](#) no Guia do usuário do Amazon Security Lake.

Etapa 1: criar um assinante do Security Lake

Você deve ser um assinante do Amazon Security Lake para consumir logs e eventos do Security Lake. Um assinante pode consultar e acessar os dados coletados pelo Security Lake. Um assinante com acesso à consulta pode consultar AWS Lake Formation tabelas diretamente em um bucket do Amazon Simple Storage Service (Amazon S3) usando serviços como o Amazon Athena. Para se tornar um assinante, o administrador do Security Lake precisa fornecer a você acesso de assinante que permita a consulta ao data lake. Para obter informações sobre como o administrador faz isso, consulte [Criação de um assinante com acesso de consulta](#) no Guia do usuário do Amazon Security Lake.

Siga estas etapas para conceder acesso de consulta a um administrador de conta do Detective.

Como criar um assinante do Detective no Security Lake

1. Abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, selecione Integrações.
3. No painel do assinante do Security Lake, observe os valores do ID da conta e do ID externo.

Peça ao administrador do Security Lake para usar esses IDs para:

- Criar um assinante do Detective para você no Security Lake.

- Fornecer acesso de consulta ao assinante.
- Para garantir que o assinante de consulta do Security Lake seja criado com as permissões do Lake Formation, selecione Lake Formation como o método de acesso aos dados no console do Security Lake.

Quando o administrador do Security Lake cria um assinante para você, o Security Lake gera um ARN do Amazon Resource Share para você. Peça ao administrador para enviar esse ARN para você.

4. Insira o ARN do compartilhamento de recursos fornecido pelo administrador do Security Lake no painel de assinante do Security Lake.
5. Depois de receber o ARN do Resource Share do administrador do Security Lake, insira o ARN na caixa ARN do compartilhamento de recursos no painel do assinante do Security Lake.

Etapa 2: adicionar as permissões necessárias do IAM à sua conta

Para habilitar a integração do Detective com o Security Lake, você deve anexar a seguinte política de permissões AWS Identity and Access Management (IAM) à sua identidade do IAM.

Anexe as políticas em linha a seguir ao perfil. Substitua `athena-results-bucket` pelo nome do bucket do Amazon S3 se quiser usar seu próprio bucket do S3 para armazenar os resultados de consulta do Athena. Se você quiser que o Detective automaticamente gere um bucket do Amazon S3 para armazenar o resultado da consulta do Athena, remova todo o `S3ObjectPermissions` da política do IAM.

Se você não tiver as permissões necessárias para anexar essa política à sua identidade do IAM, entre em contato com seu AWS administrador. Caso você tenha as permissões necessárias, mas ocorrer um problema, consulte [Solução de problemas gerais do IAM](#) no Guia do usuário do IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    }
  ]
}
```

```

    },
    {
      "Sid": "S3ObjectPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::<athena-results-bucket>",
        "arn:aws:s3:::<athena-results-bucket>/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables"
      ],
      "Resource": [
        "arn:aws:glue:*:<ACCOUNT ID>:database/amazon_security_lake*",
        "arn:aws:glue:*:<ACCOUNT ID>:table/amazon_security_lake*/
amazon_security_lake*",
        "arn:aws:glue:*:<ACCOUNT ID>:catalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:BatchGetQueryExecution",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "lakeformation:GetDataAccess",
        "ram:ListResources"
      ],
      "Resource": "*"
    },
  },

```



```

{
  "Effect": "Allow",
  "Action": [
    "ssm:GetParametersByPath"
  ],
  "Resource": [
    "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/ResourceShareArn",
    "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/S3Bucket",
    "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/TableNames",
    "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/DatabaseName",
    "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI/StackId"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "cloudformation:GetTemplateSummary",
    "iam:ListRoles"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "organizations:ServicePrincipal": [
        "securitylake.amazonaws.com"
      ]
    }
  }
}
]
}

```

Etapa 3: aceitar o convite do ARN do compartilhamento de recursos e habilitar a integração

Para acessar logs de dados brutos do Security Lake, você deve aceitar um convite do Resource Share da conta do Security Lake que foi criada pelo administrador do Security Lake. Você também precisa de permissões do AWS Lake Formation para configurar o compartilhamento de tabelas entre contas. Além disso, você deve criar um bucket do Amazon Simple Storage Service (Amazon S3) que possa receber logs de consulta brutos.

Na próxima etapa, você usará um AWS CloudFormation modelo para criar uma pilha para: aceitar o convite ARN do Resource Share, criar os recursos Crawler do AWS Glue necessários e AWS Lake Formation conceder permissões de administrador.

Para criar uma AWS CloudFormation pilha

1. Crie uma nova CloudFormation pilha usando o CloudFormation modelo. Para obter mais detalhes, consulte [Criar uma pilha usando o modelo do AWS CloudFormation](#).
2. Depois de criar a pilha, selecione Habilitar integração.

Criar uma pilha usando o modelo do AWS CloudFormation

Detective fornece um AWS CloudFormation modelo, que você pode usar para configurar os parâmetros necessários para criar e gerenciar o acesso a consultas para assinantes do Security Lake.

Etapa 1: criar uma função AWS CloudFormation de serviço

Você deve criar uma função AWS CloudFormation de serviço para criar uma pilha usando o AWS CloudFormation modelo. Se você não tiver as permissões necessárias para criar um perfil de serviço, entre em contato com o administrador da conta de administrador do Detective. Para obter mais informações sobre o perfil de serviço do AWS CloudFormation, consulte [Perfil de serviço do AWS CloudFormation](#).

1. Faça login AWS Management Console e abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação do console do IAM, escolha Roles (Perfis) e, em seguida, Create role (Criar perfil).

3. Em **Select trusted entity** (Selecionar entidade confiável), escolha **AWS Service** (Serviço).
4. Selecione **AWS CloudFormation**. Em seguida, escolha **Próximo**.
5. Insira um nome para a função. Por exemplo, **CFN-DetectiveSecurityLakeIntegration**.
6. Anexe as políticas em linha a seguir ao perfil. <Account ID>Substitua pelo ID AWS da sua conta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CloudFormationPermission",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateChangeSet"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:aws:transform/*"
      ]
    },
    {
      "Sid": "IamPermissions",
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:PutRolePolicy",
        "iam>DeleteRolePolicy",
        "iam:CreatePolicy",
        "iam>DeletePolicy",
        "iam:PassRole",
        "iam:GetRole",
        "iam:GetRolePolicy"
      ],
      "Resource": [
        "arn:aws:iam::<ACCOUNT ID>:role/*",
        "arn:aws:iam::<ACCOUNT ID>:policy/*"
      ]
    }
  ],
}
```

```

{
  "Sid": "S3Permissions",
  "Effect": "Allow",
  "Action": [
    "s3:CreateBucket",
    "s3:DeleteBucket*",
    "s3:PutBucket*",
    "s3:GetBucket*",
    "s3:GetObject",
    "s3:PutEncryptionConfiguration",
    "s3:GetEncryptionConfiguration"
  ],
  "Resource": [
    "arn:aws:s3:::*"
  ]
},
{
  "Sid": "LambdaPermissions",
  "Effect": "Allow",
  "Action": [
    "lambda:CreateFunction",
    "lambda:DeleteFunction",
    "lambda:GetFunction",
    "lambda:TagResource",
    "lambda:InvokeFunction"
  ],
  "Resource": [
    "arn:aws:lambda:*:<ACCOUNT ID>:function:*"
  ]
},
{
  "Sid": "CloudwatchPermissions",
  "Effect": "Allow",
  "Action": [
    "logs:CreateLogGroup",
    "logs:DeleteLogGroup",
    "logs:DescribeLogGroups"
  ],
  "Resource": "arn:aws:logs:*:<ACCOUNT ID>:log-group:*"
},
{
  "Sid": "KmsPermission",
  "Effect": "Allow",
  "Action": [

```

```

        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:*:<ACCOUNT ID>:key/*"
    }
  ]
}

```

Etapa 2: adicionar permissões à entidade principal do IAM.

Você precisará das seguintes permissões para criar uma pilha usando a função CloudFormation de serviço que você criou na etapa anterior. Adicione a seguinte política do IAM ao principal do IAM que você planeja usar para transmitir a função CloudFormation de serviço. Você assumirá essa entidade principal do IAM para criar a pilha. Se você não tiver as permissões necessárias para adicionar a política do IAM, entre em contato com o administrador da conta de administrador do Detective.

Note

Na política a seguir, o CFN-DetectiveSecurityLakeIntegration usado nesta política se refere ao perfil criado na etapa anterior do perfil de serviço do Creating an AWS CloudFormation. Se ele for diferente, altere-o para o nome do perfil inserido na etapa anterior.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PassRole",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::<ACCOUNT ID>:role/CFN-
DetectiveSecurityLakeIntegration"
    },
    {
      "Sid": "RestrictCloudFormationAccess",
      "Effect": "Allow",

```

```

    "Action": [
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:UpdateStack"
    ],
    "Resource": "arn:aws:cloudformation:*:<ACCOUNT ID>:stack/*",
    "Condition": {
      "StringEquals": {
        "cloudformation:RoleArn": [
          "arn:aws:iam:*:<ACCOUNT ID>:role/CFN-
DetectiveSecurityLakeIntegration"
        ]
      }
    }
  },
  {
    "Sid": "CloudformationDescribeStack",
    "Effect": "Allow",
    "Action": [
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackEvents",
      "cloudformation:GetStackPolicy"
    ],
    "Resource": "arn:aws:cloudformation:*:<ACCOUNT ID>:stack/*"
  },
  {
    "Sid": "CloudformationListStacks",
    "Effect": "Allow",
    "Action": [
      "cloudformation:ListStacks"
    ],
    "Resource": "*"
  },
  {
    "Sid": "CloudWatchPermissions",
    "Effect": "Allow",
    "Action": [
      "logs:GetLogEvents"
    ],
    "Resource": "arn:aws:logs:*:<ACCOUNT ID>:log-group:*"
  }
]
}

```

Etapa 3: especificar valores personalizados no AWS CloudFormation console

1. Vá para o AWS CloudFormation console do Detective.
2. (Opcional) Insira o nome da pilha. O nome da pilha é preenchido automaticamente. Você pode alterar o nome da pilha desde que o nome não entre em conflito com os nomes de pilhas existentes.
3. Insira os seguintes parâmetros.
 - AthenaResultsBucket— Se você não inserir valores, esse modelo gerará um bucket do Amazon S3. Se você quiser usar seu próprio bucket, insira um nome de bucket para armazenar os resultados da consulta do Athena. Se você usar seu próprio bucket, verifique se ele está na mesma região do ARN do compartilhamento de recursos. Se você usar seu próprio bucket, garanta que o LakeFormationPrincipals escolhido tenha permissões para gravar e ler objetos do bucket. Para obter mais detalhes sobre as permissões do bucket, consulte [Resultados de consultas e consultas recentes](#) no Guia do usuário do Amazon Athena.
 - DTRegion: este campo é pré-preenchido. Não altere os valores desse campo.
 - LakeFormationPrincipals— Insira o ARN dos diretores do IAM (por exemplo, ARN da função do IAM) aos quais você deseja conceder acesso para usar a integração do Security Lake, separados por vírgulas. Esses podem ser seus analistas de segurança e engenheiros de segurança que usam o Detective.

Só é possível usar as entidades principais do IAM anteriormente anexadas às permissões do IAM na etapa [Step 2: Add the required IAM permissions to your account].
 - ResourceShareARN — Esse campo está pré-preenchido. Não altere os valores desse campo.
4. Permissões

Perfil do IAM: selecione o perfil criado na etapa *Creating an AWS CloudFormation Service Role*. Como opção, você pode manter esse campo em branco se o perfil do IAM atual tiver todas as permissões necessárias na etapa *Creating an AWS CloudFormation Service Role*.
5. Revise e marque todas as caixas *Eu confirmo e*, em seguida, clique no botão *Criar pilha*. Para obter mais detalhes, revise os recursos do IAM a seguir que serão criados.

* ResourceShareAcceptorCustomResourceFunction
- ResourceShareAcceptorLambdaRole

```

- ResourceShareAcceptorLogsAccessPolicy
* SsmParametersCustomResourceFunction
  - SsmParametersLambdaRole
  - SsmParametersLogsAccessPolicy
* GlueDatabaseCustomResourceFunction
  - GlueDatabaseLambdaRole
  - GlueDatabaseLogsAccessPolicy
* GlueTablesCustomResourceFunction
  - GlueTablesLambdaRole
  - GlueTablesLogsAccessPolicy

```

Etapa 4: adicionar a política de bucket do Amazon S3 às entidades principais do IAM em **LakeFormationPrincipals**

(Opcional) Se você permitir que o modelo gere um AthenaResultsBucket, você deve anexar a política a seguir às entidades principais do IAM em LakeFormationPrincipals.

```

{
  "Sid": "S3ObjectPermissions",
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::<athena-results-bucket>",
    "arn:aws:s3:::<athena-results-bucket>/*"
  ]
}

```

athena-results-bucketSubstitua pelo AthenaResultsBucket nome. Eles AthenaResultsBucket podem ser encontrados no AWS CloudFormation console:

1. Abra o AWS CloudFormation console em <https://console.aws.amazon.com/cloudformation>.
2. Clique na pilha.
3. Clique na guia Recursos.
4. Busque o ID lógico AthenaResultsBucket e copie seu ID físico.

Excluindo uma pilha CloudFormation

Se você não excluir a pilha existente, a criação da nova pilha na mesma região falhará. Você pode excluir uma CloudFormation pilha usando o CloudFormation console ou a AWS CLI.

Para excluir a AWS CloudFormation pilha (Console)

1. Abra o AWS CloudFormation console em <https://console.aws.amazon.com/cloudformation>.
2. Na página Pilhas no CloudFormation console, selecione a pilha que você deseja excluir. A pilha deve estar em execução no momento.
3. No painel de detalhes da pilha, escolha Excluir.
4. Selecione Excluir pilha quando solicitado.

Note

A operação de exclusão da pilha não pode ser interrompida uma vez que a ação já tenha começado. A pilha continua para o estado DELETE_IN_PROGRESS.

Quando a exclusão da pilha for concluída, a pilha estará no estado DELETE_COMPLETE.

Solução de problemas de erros na exclusão da pilha

Se você estiver vendo um erro de permissão com a mensagem `Failed to delete stack` depois de clicar no Delete botão, sua função do IAM não tem CloudFormation permissão para excluir uma pilha. Entre em contato com o administrador da conta para excluir a pilha.

Para excluir a CloudFormation pilha (AWS CLI)

Digite o seguinte comando na interface AWS CLI:

```
aws cloudformation delete-stack --stack-name your-stack-name --role-arn
arn:aws:iam::<ACCOUNT ID>:role/CFN-DetectiveSecurityLakeIntegration
```

O `CFN-DetectiveSecurityLakeIntegration` é o perfil de serviço criado na etapa `Creating an AWS CloudFormation Service Role`.

Alterar a configuração da integração

Se quiser alterar qualquer um dos parâmetros usados para integrar o Detective ao Security Lake, você pode editá-los e, em seguida, habilitar a integração novamente. Você pode editar o AWS CloudFormation modelo para reativar essa integração nos seguintes cenários:

- Para atualizar a assinatura do Security Lake, você pode criar um novo assinante ou o administrador do Security Lake pode atualizar a fonte de dados da assinatura existente.
- Especificar um bucket do Amazon S3 diferente para armazenar os logs de consulta brutos.
- Especificar diferentes entidades principais do Lake Formation.

Ao habilitar novamente a integração do Detective ao Security Lake, é possível editar o ARN do compartilhamento de recursos e visualizar as Permissões do IAM. Acesse o console do IAM no Detective para editar as permissões do IAM. Você também pode editar os valores inseridos anteriormente no AWS CloudFormation modelo. Você deve excluir a CloudFormation pilha existente e recriá-la para reativar a integração.

Como reabilitar a integração do Detective ao Security Lake

1. Abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, selecione Integrações.
3. Você pode editar a integração usando uma destas etapas:
 - No painel Security Lake, selecione Editar.
 - No painel Security Lake, selecione Exibir. Na página de visualização, selecione Editar.
4. Insira um novo ARN de Resource Share para acessar as fontes de dados em uma região.
5. Visualize as permissões atuais do IAM e acesse o console do IAM se quiser editá-las.
6. Edite os valores no CloudFormation modelo.
 1. Antes de criar uma nova pilha, primeiro exclua a pilha existente. Se você não excluir a pilha existente e tentar criar uma nova pilha na mesma região, a solicitação falhará. Para obter mais detalhes, consulte [Excluindo uma pilha CloudFormation](#).
 1. Crie uma nova CloudFormation pilha. Para obter mais detalhes, consulte [Criar uma pilha usando o modelo do AWS CloudFormation](#).
7. Selecione Habilitar integração.

Desabilitar a integração

Se você desabilitar a integração do Detective ao Security Lake, não poderá mais consultar dados de log e eventos do Security Lake.

Como desabilitar a integração do Detective ao Security Lake

1. Abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, selecione Integrações.
3. Exclua a pilha existente. Para obter mais detalhes, consulte [Excluindo uma pilha CloudFormation](#).
4. No painel Desabilitar a integração ao Security Lake, selecione Desabilitar.

AWS Regiões suportadas

Você pode integrar o Detective com o Security Lake nas seguintes AWS regiões.

Nome da região	Região	Endpoint	Protocolo
Leste dos EUA (Ohio)	us-east-2	securitylake.us-east-2.amazonaws.com	HTTPS
Leste dos EUA (Norte da Virgínia)	us-east-1	securitylake.us-east-1.amazonaws.com	HTTPS
Oeste dos EUA (Norte da Califórnia)	us-west-1	securitylake.us-west-1.amazonaws.com	HTTPS
Oeste dos EUA (Oregon)	us-west-2	securitylake.us-west-2.amazonaws.com	HTTPS
Ásia-Pacífico (Mumbai)	ap-south-1	securitylake.ap-south-1.amazonaws.com	HTTPS
Ásia-Pacífico (Seul)	ap-northeast-2	securitylake.ap-northeast-2.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
Ásia-Pacífico (Singapura)	ap-southeast-1	securitylake.ap-southeast-1.amazonaws.com	HTTPS
Ásia-Pacífico (Sydney)	ap-southeast-2	securitylake.ap-southeast-2.amazonaws.com	HTTPS
Ásia-Pacífico (Tóquio)	ap-northeast-1	securitylake.ap-northeast-1.amazonaws.com	HTTPS
Canadá (Central)	ca-central-1	securitylake.ca-central-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	securitylake.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	securitylake.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	securitylake.eu-west-2.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	securitylake.eu-west-3.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	securitylake.eu-north-1.amazonaws.com	HTTPS
América do Sul (São Paulo)	sa-east-1	securitylake.sa-east-1.amazonaws.com	HTTPS

Consultar logs brutos no Detective

Depois de integrar o Detective ao Security Lake, o Detective começa a extrair registros brutos do Security Lake relacionados a eventos de AWS CloudTrail gerenciamento e aos registros de fluxo da Amazon Virtual Private Cloud (Amazon VPC).

Note

Não há cobranças adicionais pela consulta de logs brutos no Detective. As taxas de uso de outros AWS Serviços, incluindo o Amazon Athena, ainda se aplicam às tarifas publicadas.

AWS CloudTrail os eventos de gerenciamento estão disponíveis para os seguintes perfis:

- AWS conta
- AWS usuário
- AWS papel
- AWS função: Sessão
- Instância do Amazon EC2
- Bucket do Amazon S3
- Endereço IP
- Cluster Kubernetes
- Cápsula Kubernetes
- Assunto do Kubernetes
- IAM role (Perfil do IAM)
- Sessão de função do IAM
- IAM user (Usuário do IAM)

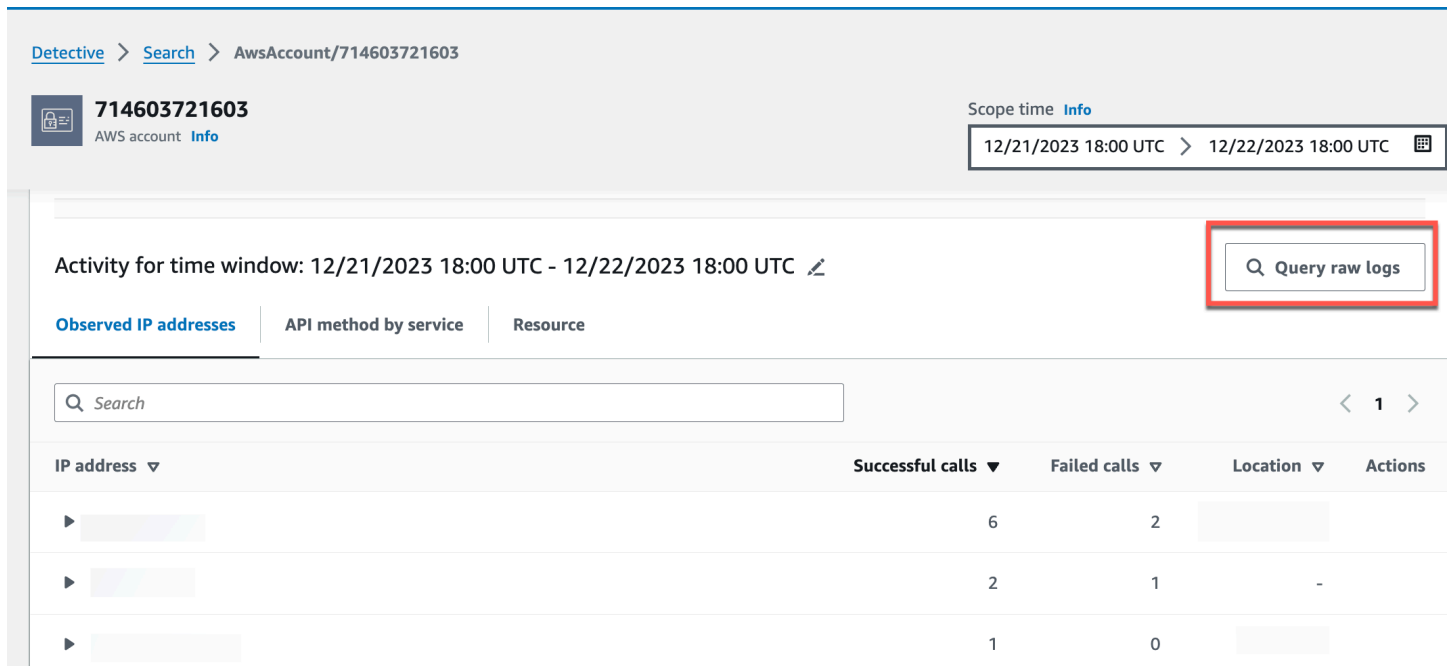
Os logs de fluxo do Amazon VPC estão disponíveis para os seguintes perfis:

- Instância do Amazon EC2
- Pod do Kubernetes

Para uma demonstração de como integrar o Amazon Detective com o Amazon Security Lake usando o console Detective, assista ao seguinte vídeo: [Integração do Amazon Detective com o Amazon Security Lake- Como usar -->](#)

Como consultar logs brutos de uma conta da AWS

1. Abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, selecione Pesquisar e procure uma AWS account.
3. Na seção Volume geral de chamadas de API, selecione os detalhes de exibição para o tempo de escopo.
4. Neste ponto, você pode começar a Consultar logs brutos.



The screenshot shows the Amazon Detective console interface. At the top, there is a breadcrumb trail: [Detective](#) > [Search](#) > [AwsAccount/714603721603](#). Below this, the account ID **714603721603** is displayed as an 'AWS account' with an 'Info' link. To the right, the 'Scope time' is set to '12/21/2023 18:00 UTC' to '12/22/2023 18:00 UTC'. The main content area shows 'Activity for time window: 12/21/2023 18:00 UTC - 12/22/2023 18:00 UTC'. Below this, there are three tabs: 'Observed IP addresses' (selected), 'API method by service', and 'Resource'. A search bar is present above a table. A red box highlights a button labeled 'Query raw logs' in the top right corner of the activity area. The table below has columns for 'IP address', 'Successful calls', 'Failed calls', 'Location', and 'Actions'. It contains three rows of data:

IP address	Successful calls	Failed calls	Location	Actions
[Redacted]	6	2	[Redacted]	
[Redacted]	2	1	-	
[Redacted]	1	0	[Redacted]	

Na tabela de Visualização do log bruto, é possível visualizar os logs e eventos recuperados consultando dados do Security Lake. Para obter mais detalhes sobre os logs de eventos brutos, você pode visualizar os dados exibidos no Amazon Athena.

Raw log preview: CloudTrail



View raw event logs that were retrieved by querying data from Security Lake. For more details about the raw event logs, you can view the data displayed in Athena.

Raw log preview (500+)							< 1 2 3 4 5 6 7 ... 50 >
date_time	requestor_arn	account_id	region	source_ip	service	api_	
2023-12-22 09:58:38.000 UTC			us-east-1		s3.amazonaws.com	GetE	
2023-12-22 09:59:49.000 UTC			us-east-1		sts.amazonaws.com	Assu	
2023-12-22 10:00:13.000 UTC			us-east-1		ec2.amazonaws.com	Desc	
2023-12-22 10:00:13.000 UTC			us-east-1		sts.amazonaws.com	Assu	
2023-12-22 10:00:13.000 UTC			us-east-1		iam.amazonaws.com	GetI	
2023-12-22 10:00:13.000 UTC			us-east-1		sts.amazonaws.com	Assu	
2023-12-22 10:00:13.000 UTC			us-east-1		sts.amazonaws.com	GetC	
2023-12-22 10:00:13.000 UTC			us-east-1		autoscaling.amazonaws.com	Desc	
2023-12-22 10:00:14.000 UTC			us-east-1		ec2.amazonaws.com	Desc	
2023-12-22 10:00:14.000 UTC			us-east-1		ec2.amazonaws.com	Desc	

Close

Cancel query request

See results in Athena

Download results

Na tabela Consultar logs brutos, você pode Cancelar solicitação de consulta, Ver resultados no Amazon Athena e Baixar resultados como um arquivo de valores separados por vírgula (.csv).

Se você ver logs no Detective, mas a consulta não retornou nenhum resultado, existem alguns motivos pelos quais isso pode ter acontecido.

- Os logs brutos podem ficar disponíveis no Detective antes de aparecerem nas tabelas de log do Security Lake. Tente novamente mais tarde.
- Os logs podem estar ausentes do Security Lake. Se você esperou por um longo período, isso indica que faltam logs do Security Lake. Entre em contato com o administrador do Security Lake para resolver o problema.

Exemplos

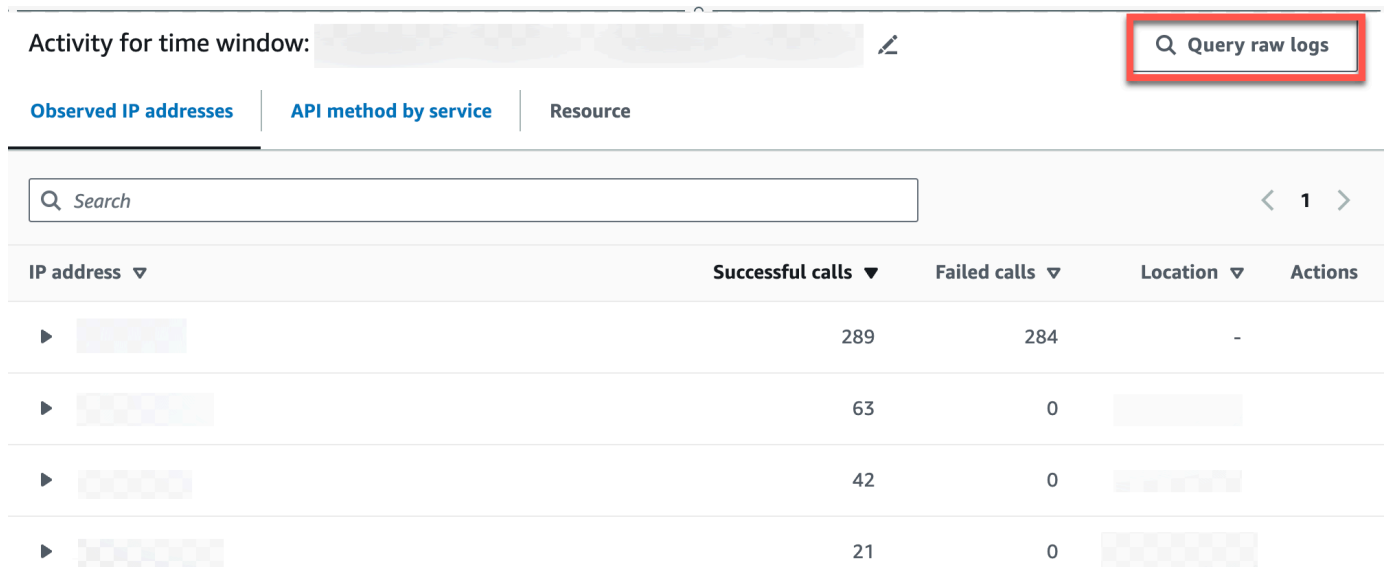
- [Consulte registros brutos para uma AWS função](#)
- [Consulte registros brutos para um cluster Amazon EKS](#)
- [Consultar logs brutos de uma instância do Amazon EC2](#)

Consulte registros brutos para uma AWS função

Se quiser entender a atividade de uma AWS função em uma nova geolocalização, você pode fazer isso no console do Detective.

Como consultar logs brutos de um perfil da AWS

1. Abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. Na página Resumo do Detective, seção Geolocalizações recém-observadas, anote a função AWS.
3. No painel de navegação, selecione Pesquisar e procure pelo AWS role.
4. Para a AWS função, expanda o recurso para exibir as chamadas de API específicas que foram emitidas desse endereço IP por esse recurso.
5. Selecione o ícone de lupa ao lado da chamada de API que você deseja investigar para abrir a tabela de Visualização do log bruto.



The screenshot shows the Amazon Detective console interface. At the top, there is a search bar with the text 'Activity for time window:'. To the right of this bar is a button labeled 'Query raw logs' with a magnifying glass icon, which is highlighted with a red rectangular box. Below the search bar, there are three tabs: 'Observed IP addresses' (selected), 'API method by service', and 'Resource'. Underneath the tabs is another search bar with the text 'Search'. To the right of this search bar are navigation arrows and the number '1'. Below these elements is a table with the following columns: 'IP address', 'Successful calls', 'Failed calls', 'Location', and 'Actions'. The table contains four rows of data, each with a play button icon on the left.

IP address ▾	Successful calls ▾	Failed calls ▾	Location ▾	Actions
▶ [redacted]	289	284	-	
▶ [redacted]	63	0	[redacted]	
▶ [redacted]	42	0	[redacted]	
▶ [redacted]	21	0	[redacted]	

Consulte registros brutos para um cluster Amazon EKS

1. Abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. Na página Resumo do Detective, seção Clusters de contêineres com a maioria dos pods criados, navegue até um cluster do Amazon EKS.
3. Na página de detalhes do cluster do Amazon EKS, selecione a guia Atividade da API Kubernetes.

- Na seção Atividade geral da API Kubernetes envolvendo esse cluster do Amazon EKS, escolha exibir detalhes para o tempo do escopo.
- Neste ponto, você pode começar a Consultar logs brutos.

Consultar logs brutos de uma instância do Amazon EC2

- Abra o console do Detective em <https://console.aws.amazon.com/detective/>.
- No painel de navegação, selecione Pesquisar e procure uma Amazon EC2 instance.
- Na seção Volume de fluxo geral da VPC, selecione o ícone de lupa ao lado da chamada de API que você deseja investigar para abrir a tabela de Visualização do log bruto.
- Neste ponto, você pode começar a Consultar logs brutos.

Activity for time window: 11/21/2023 11:00 (UTC-08:00) - 11/22/2023 11:00 (UTC-08:00) Toggle overall traffic Query raw logs

< 1 2 3 4 5 6 7 ... 888 >

<input type="checkbox"/>	IP address	Local port	Remote port	Inbound traffic	Outbound traffic	Protocol	Directionality	Accept / Reject	Actions
<input type="checkbox"/>		22	-	44.7 kB	57.7 kB	TCP	Inbound	Accept	<input type="text" value="Q"/>
<input type="checkbox"/>		22	-	240 B	480 B	TCP	Inbound	Accept	<input type="text" value="Q"/>
<input type="checkbox"/>		22	-	61.1 kB	75 kB	TCP	Inbound	Accept	<input type="text" value="Q"/>
<input type="checkbox"/>		22	-	59.6 kB	70.8 kB	TCP	Inbound	Accept	<input type="text" value="Q"/>
<input type="checkbox"/>		22	-	240 B	540 B	TCP	Inbound	Accept	<input type="text" value="Q"/>

Na tabela de Visualização do log bruto, é possível visualizar os logs e eventos recuperados consultando dados do Security Lake. Para obter mais detalhes sobre os logs de eventos brutos, você pode visualizar os dados exibidos no Amazon Athena.

Na tabela Consultar logs brutos, você pode Cancelar solicitação de consulta, Ver resultados no Amazon Athena e Baixar resultados como um arquivo de valores separados por vírgula (.csv).

Segurança no Amazon Detective

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.

Audidores 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 que se aplicam ao Amazon Detective, consulte [Serviços da AWS 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 a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Detective. Os tópicos a seguir mostram como configurar o Detective para atender aos seus objetivos de segurança e conformidade. Você também aprende a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos de Detective.

Conteúdo

- [Proteção de dados no Amazon Detective](#)
- [Gerenciamento de identidade e acesso para o Amazon Detective](#)
- [Registro e monitoramento no Amazon Detective](#)
- [Validação de compatibilidade do Amazon Detective](#)
- [Resiliência no Amazon Detective](#)
- [Segurança da infraestrutura no Amazon Detective](#)
- [Práticas recomendadas de segurança para o Amazon Detective](#)

Proteção de dados no Amazon Detective

O [modelo de responsabilidade AWS compartilhada](#) se aplica à proteção de dados no Amazon Detective. 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 o Detective ou outro Serviços da AWS usando o console, a API ou AWS os AWS CLI SDKs. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de

diagnóstico. Se você fornecer um URL para um servidor externo, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

O Detective criptografa todos os dados que processa e armazena em repouso e em trânsito.

Conteúdo

- [Gerenciamento de chaves do Amazon Detective](#)

Gerenciamento de chaves do Amazon Detective

Como o Detective não armazena nenhum dado de identificação pessoal do cliente, ele usa Chaves gerenciadas pela AWS.

Esse tipo de chave KMS pode ser usado em várias contas. Veja a [descrição das chaves AWS próprias no Guia do AWS Key Management Service desenvolvedor](#).

Esse tipo de chave KMS alterna automaticamente a cada ano (aproximadamente 365 dias). Veja a [descrição da rotação de chaves no Guia do AWS Key Management Service desenvolvedor](#).

Gerenciamento de identidade e acesso para o Amazon Detective

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 (fazer login) e autorizado (ter permissões) para usar os recursos do Detective. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Conteúdo

- [Público](#)
- [Autenticação com identidades](#)
- [Gerenciamento do acesso usando políticas](#)
- [Como o Amazon Detective funciona com o IAM](#)
- [Exemplos de políticas baseadas em identidade do Amazon Detective](#)
- [AWS políticas gerenciadas para o Amazon Detective](#)
- [Usar funções vinculadas ao serviço do Detective](#)
- [Solução de problemas de identidade e acesso do Amazon Detective](#)

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Detective.

Usuário do serviço: se você usa o serviço do Detective para fazer o trabalho, o administrador fornece as credenciais e as permissões necessárias. À medida que usar mais recursos do Detective para fazer o trabalho, você precisará de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um recurso no Detective, consulte [Solução de problemas de identidade e acesso do Amazon Detective](#).

Administrador do serviço: se você for o responsável pelos recursos do Detective na empresa, provavelmente terá acesso total ao Detective. Cabe a você determinar quais funcionalidades e recursos do Detective os 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 a empresa pode usar o IAM com o Detective, consulte [Como o Amazon Detective funciona com o IAM](#).

Administrador do IAM: se você for um administrador do IAM, poderá saber detalhes sobre como é possível criar políticas para gerenciar o acesso ao Detective. Para visualizar exemplos de políticas baseadas em identidade do Detective que podem ser usadas no IAM, consulte [Exemplos de políticas baseadas em identidade do Amazon Detective](#).

Autenticação com identidades

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

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como uma identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login 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.

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 [Altere as chaves de acesso regularmente para casos de uso que exijam credenciais](#) de longo prazo no Guia do usuário do IAM.

Um [grupo do IAM](#) é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e atribuir a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis.. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte [Quando criar um usuário do IAM \(em vez de uma função\)](#) 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](#) no AWS 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 (um principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recurso para acesso entre contas, consulte [Como as funções do IAM](#) diferem das políticas baseadas em recurso no Guia do usuário do IAM.
- **Acesso entre serviços** — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso

usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.

- Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado 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](#).
- Função de serviço: uma função 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 o perfil para executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.
- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. É preferível fazer isso e armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para 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 uma função 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 embutidas são anexadas diretamente a um único usuário, grupo ou função. 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 recurso

Políticas baseadas em recurso são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil 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 recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve [especificar uma entidade principal](#) em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha 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 (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade e dos seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou a função no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte [Limites de permissões para identidades do IAM](#) no Guia do usuário do IAM.
- **Políticas de controle de serviço (SCPs)** — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS que sua empresa possui. Se você habilitar todos os 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 [How SCPs work \(Como os SCPs funcionam\)](#) no AWS Organizations Guia do usuário do .

- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para uma função ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recurso. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para 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 o Amazon Detective funciona com o IAM

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do Amazon Detective. Eles também não podem realizar tarefas usando a AWS API AWS Management Console AWS CLI, ou. Um administrador de Detective deve ter políticas AWS Identity and Access Management (IAM) que concedam permissão aos usuários e funções do IAM para realizar operações de API específicas nos recursos especificados de que precisam. O administrador deve anexar essas políticas às entidades principais que exigem essas permissões.

O Detective usa políticas baseadas em identidade do IAM para conceder permissões para os seguintes tipos de usuários e ações:

- Contas de administrador: a conta de administrador é proprietária de um gráfico de comportamento, que usa dados de sua conta. Uma conta de administrador pode convidar contas-membro para contribuírem com seus dados no gráfico de comportamento. A conta do administrador também pode usar o gráfico de comportamento para triagem e investigação de descobertas e recursos associados a essas contas.

Você pode configurar políticas para permitir que usuários que não sejam a conta de administrador realizem diferentes tipos de tarefas. Por exemplo, um usuário de uma conta de administrador pode

ter permissões apenas para gerenciar contas-membro. Outro usuário pode ter permissão apenas para usar o gráfico de comportamento para investigação.

- **Contas-membro:** uma conta-membro é uma conta convidada a contribuir com dados em um gráfico de comportamento. A conta-membro responde a um convite. Depois de aceitar um convite, a conta-membro pode remover a própria conta do gráfico de comportamento.

Para ter uma visão geral de como o Detective e Serviços da AWS outros trabalham com o IAM, [consulte Criação de políticas na guia JSON no Guia do usuário do IAM](#).

Políticas baseadas em identidade do Detective

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. O Detective oferece suporte a ações, recursos e chaves de condição específicos.

Para conhecer todos os elementos usados em uma política JSON, consulte [Referência de elementos de política JSON do IAM](#) no Guia do usuário do IAM.

Ações

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

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

As instruções de política devem incluir um elemento `Action` ou `NotAction`. O elemento `Action` lista as ações permitidas pela política. O elemento `NotAction` lista as ações que não são permitidas.

As ações definidas para o Detective refletem as tarefas que você pode realizar usando o Detective. As ações das políticas no Detective têm o seguinte prefixo: `detective:`.

Por exemplo, para conceder permissão para usar a operação da API `CreateMembers` e convidar contas-membro para um gráfico de comportamento, inclua a ação `detective:CreateMembers` na política.

Para especificar várias ações em uma única instrução, separe-as com vírgulas. Por exemplo, para uma conta-membro, a política inclui o conjunto de ações relacionadas ao gerenciamento de um convite:

```
"Action": [
    "detective:ListInvitations",
    "detective:AcceptInvitation",
    "detective:RejectInvitation",
    "detective:DisassociateMembership"
]
```

Você também pode usar curingas (*) para especificar várias ações. Por exemplo, para gerenciar os dados usados no gráfico de comportamento, as contas de administrador no Detective devem conseguir realizar as seguintes tarefas:

- Visualizar a lista de contas-membro (`ListMembers`).
- Obter informações sobre as contas-membro selecionadas (`GetMembers`).
- Convidar contas-membro para o gráfico de comportamento (`CreateMembers`).
- Remover membros do gráfico de comportamento (`DeleteMembers`).

Em vez de listar essas ações separadamente, você pode conceder acesso a todas as ações que terminam com a palavra `Members`. A política para isso pode incluir a seguinte ação:

```
"Action": "detective:*Members"
```

Para ver uma lista das ações do Detective, consulte [Ações definidas pelo Amazon Detective](#) na Referência de autorização do serviço.

Recursos

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 seu [nome do recurso da Amazon \(ARN\)](#). Isso pode ser feito para ações que oferecem suporte a um tipo de recurso específico, conhecido como permissões em nível de recurso.

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

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

Para obter mais informações sobre o formato dos ARNs, consulte [Amazon Resource Names \(ARNs\) e AWS Service Namespaces](#).

Para o Detective, o único tipo de recurso é o gráfico de comportamento. O recurso de gráfico de comportamento do Detective tem o seguinte ARN:

```
arn:aws:detective:${Region}:${AccountId}:graph:${GraphId}
```

Por exemplo, um gráfico de comportamento tem os seguintes valores:

- A região do gráfico de comportamento é `us-east-1`.
- A ID de conta da conta de administrador é `111122223333`.
- A ID de gráfico do gráfico de comportamento é `027c7c4610ea4aacf0b883093cab899`.

Para identificar esse gráfico de comportamento em uma instrução `Resource`, você deve usar o seguinte ARN:

```
"Resource": "arn:aws:detective:us-east-1:111122223333:graph:027c7c4610ea4aacf0b883093cab899"
```

Para especificar vários recursos em uma instrução `Resource`, separe-os com vírgulas.

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

Por exemplo, a mesma AWS conta pode ser convidada para ser uma conta de membro em mais de um gráfico de comportamento. Na política dessa conta-membro, a instrução `Resource` lista os gráficos de comportamento para os quais foram convidadas.

```
"Resource": [  
    "arn:aws:detective:us-east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",  
    "arn:aws:detective:us-east-1:444455556666:graph:056d2a9521xi2bb1uw1d164680eby416"  
]
```

Algumas ações do Detective, como criar um gráfico de comportamento, listar gráficos de comportamento e listar convites para gráficos de comportamento, não são executadas em um gráfico de comportamento específico. Para essas ações, a instrução `Resource` deve usar o caractere curinga (*).

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

Para ações da conta de administrador, o Detective sempre verifica se o usuário que fez a solicitação pertence à conta de administrador do gráfico de comportamento afetado. Para ações da conta-membro, o Detective sempre verifica se o usuário que fez a solicitação pertence à conta-membro. Mesmo que uma política do IAM conceda acesso a um gráfico de comportamento, se o usuário não pertencer à conta correta, ele não poderá realizar a ação.

Para todas as ações executadas em um gráfico de comportamento específico, a política do IAM deve incluir o ARN do gráfico. O ARN do gráfico pode ser adicionado posteriormente. Por exemplo, quando uma conta habilita o Detective pela primeira vez, a política inicial do IAM fornece acesso a todas as ações do Detective usando o caractere curinga para o ARN do gráfico. Isso permite que o usuário comece imediatamente a gerenciar as contas-membro e conduzir investigações em seu gráfico de comportamento. Depois que o gráfico de comportamento for criado, você poderá atualizar a política para adicionar o ARN do gráfico.

Chaves de condição

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 recurso 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.

O Detective não define seu próprio conjunto de chaves de condição. Ele oferece suporte ao uso de algumas chaves de condição globais. Para ver todas as chaves de condição AWS globais, consulte [Chaves de contexto de condição AWS global](#) no Guia do usuário do IAM.

Para saber com quais ações e recursos é possível usar a chave de condição, consulte [Ações definidas pelo Amazon Detective](#).

Exemplos

Para visualizar exemplos de políticas baseadas em identidade do Detective, consulte [Exemplos de políticas baseadas em identidade do Amazon Detective](#).

Políticas baseadas em recurso do Detective (não compatíveis)

O Detective não oferece suporte a políticas baseadas em recurso.

Autorização baseada em tags dos gráficos de comportamento do Detective

Cada gráfico de comportamento pode receber valores de tag. Você pode usar esses valores de tag em instruções condicionais para gerenciar o acesso ao gráfico de comportamento.

A instrução condicional para um valor de tag usa o formato a seguir.


```
{"StringEquals":{"aws:ResourceTag/<tagName>": "<tagValue>"}}
```

Por exemplo, use o código a seguir para permitir ou negar uma ação quando o valor da tag Department for Finance.

```
{"StringEquals":{"aws:ResourceTag/Department": "Finance"}}
```

Para ver exemplos de políticas que usam valores de tag de recurso, consulte [the section called “Conta de administrador: restringir o acesso com base em valores de tag”](#).

Perfis do IAM no Detective

Uma [função do IAM](#) é uma entidade dentro da sua AWS conta que tem permissões específicas.

Usar credenciais temporárias com o Detective

É possível usar credenciais temporárias para fazer login com federação, assumir um perfil do IAM ou assumir um perfil entre contas. Você obtém credenciais de segurança temporárias chamando operações de AWS STS API, como [AssumeRole](#) ou [GetFederationToken](#).

O Detective oferece suporte ao uso de credenciais temporárias.

Funções vinculadas ao serviço

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

Para obter detalhes sobre como criar ou gerenciar funções vinculadas ao serviço do Detective, consulte [the section called “Usar funções vinculadas a serviços”](#).

Perfis de serviço (não compatíveis)

Esse atributo permite que um serviço assuma um [perfil de serviço](#) em seu nome. O perfil permite que o serviço acesse recursos em outros serviços para concluir uma ação em seu nome. Os perfis de serviço aparecem em sua conta do IAM e são de propriedade da conta. Isso indica que um administrador do IAM pode alterar as permissões para essa função. Porém, fazer isso pode alterar a funcionalidade do serviço.

O Detective não é compatível com perfis de serviço.

Exemplos de políticas baseadas em identidade do Amazon Detective

Por padrão, os usuários e perfis do IAM não têm permissão para criar ou modificar recursos do Detective. Eles também não podem realizar tarefas usando a AWS API, a AWS Management Console, a AWS CLI, ou.

Um administrador do IAM deve criar políticas do IAM que concedam aos usuários e perfis permissão para executarem operações de API específicas nos recursos especificados de que precisam. O administrador deve anexar essas políticas aos usuários ou grupos do IAM que exigem essas permissões.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documentos de política JSON, consulte [Criar políticas na guia JSON](#) no Guia do usuário do IAM.

Tópicos

- [Melhores práticas de política](#)
- [Usar o console do Detective](#)
- [Permitir que os usuários visualizem suas próprias permissões](#)
- [Conta de administrador: gerenciar as contas-membro em um gráfico de comportamento](#)
- [Conta de administrador: usar um gráfico de comportamento para investigação](#)
- [Contas-membro: gerenciar convites e associações a gráficos de comportamento](#)
- [Conta de administrador: restringir o acesso com base em valores de tag](#)

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Detective 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 avance 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 [AWS Políticas gerenciadas](#) pela [AWS ou Políticas gerenciadas pela para funções](#) 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 recursos 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 recursos. 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.

Usar o console do Detective

Para usar o console do Amazon Detective, o usuário ou a função devem ter acesso às ações relevantes, que se igualam às ações correspondentes na API.

Para habilitar o Detective e se tornar uma conta de administrador de um gráfico de comportamento, o usuário ou a função deve ter permissão para a ação `CreateGraph`.

Para usar o console do Detective para realizar qualquer ação na conta de administrador, o usuário ou a função deve ter permissão para a ação `ListGraphs`. Isso concede permissão para recuperar os gráficos de comportamento dos quais sua conta é uma conta de administrador. Também devem receber permissão para realizar ações específicas da conta de administrador.

As ações mais básicas da conta de administrador são visualizar uma lista de contas-membro em um gráfico de comportamento e usar o gráfico de comportamento para investigação.

- Para visualizar a lista de contas-membro em um gráfico de comportamento, a entidade principal deve ter permissão para a ação `ListMembers`.
- Para conduzir uma investigação em um gráfico de comportamento, a entidade principal deve ter permissão para a ação `SearchGraph`.

Para usar o console do Detective para realizar qualquer ação em uma conta-membro, o usuário ou a função deve ter permissão para a ação `ListInvitations`. Isso concede permissão para visualizar convites para gráficos de comportamento. Em seguida, podem receber permissão para ações específicas da conta-membro.

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:ListGroupsWithUser",
        "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": "*"
    }
  ]
}

```

Conta de administrador: gerenciar as contas-membro em um gráfico de comportamento

Este exemplo de política é destinado a usuários de contas de administrador que são responsáveis somente pelo gerenciamento das contas-membro usadas no gráfico de comportamento. A política também permite que o usuário visualize as informações de uso e desabilite o Detective. A política não concede permissão para usar o gráfico de comportamento para investigação.

```

{"Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":
      ["detective:ListMembers","detective:CreateMembers","detective:DeleteMembers","detective:DeleteG",
        "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
      ],
    },
    {
      "Effect":"Allow",
      "Action":["detective:CreateGraph","detective:ListGraphs"],
      "Resource":"*"
    }
  ]
}

```

Conta de administrador: usar um gráfico de comportamento para investigação

Este exemplo de política é destinado a usuários de contas de administrador que usam o gráfico de comportamento somente para investigação. Eles não podem visualizar ou editar a lista de contas-membro no gráfico de comportamento.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["detective:SearchGraph"],
      "Resource": "arn:aws:detective:us-east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
    },
    {
      "Effect": "Allow",
      "Action": ["detective:ListGraphs"],
      "Resource": "*"
    }
  ]
}
```

Contas-membro: gerenciar convites e associações a gráficos de comportamento

Este exemplo de política é destinado a usuários pertencentes a uma conta-membro. No exemplo, a conta-membro pertence a dois gráficos de comportamento. A política concede permissão para responder aos convites e remover a conta-membro do gráfico de comportamento.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation", "detective:RejectInvitation", "detective:DisassociateMembership"
      ],
      "Resource": [
        "arn:aws:detective:us-east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
        "arn:aws:detective:us-east-1:444455556666:graph:056d2a9521xi2bb1uw1d164680eby416"
      ]
    },
    {

```

```

    "Effect": "Allow",
    "Action": ["detective:ListInvitations"],
    "Resource": "*"
  }
]
}

```

Conta de administrador: restringir o acesso com base em valores de tag

A política a seguir permite que o usuário use um gráfico de comportamento para investigação se a tag `SecurityDomain` do gráfico de comportamento corresponder à tag `SecurityDomain` do usuário.

```

{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Allow",
    "Action": ["detective:SearchGraph"],
    "Resource": "arn:aws:detective:*:*:graph:*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/SecurityDomain": "aws:PrincipalTag/SecurityDomain"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": ["detective:ListGraphs"],
    "Resource": "*"
  } ]
}

```

A política a seguir permite que os usuários usem um gráfico de comportamento para investigação se o valor da tag `SecurityDomain` do gráfico de comportamento for `Finance`.

```

{
  "Version": "2012-10-17",
  "Statement": [ {
    "Effect": "Deny",
    "Action": ["detective:SearchGraph"],
    "Resource": "arn:aws:detective:*:*:graph:*",
    "Condition": {

```

```
        "StringEquals": {"aws:ResourceTag/SecurityDomain": "Finance"}
    }
} ]
}
```

AWS políticas gerenciadas para o Amazon Detective

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

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo [políticas gerenciadas pelo cliente](#) específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) for lançada ou novas operações de API forem disponibilizadas para serviços existentes.

Para mais informações, consulte [Políticas gerenciadas pela AWS](#) no Manual do usuário do IAM.

AWS política gerenciada: AmazonDetectiveFullAccess

É possível anexar a política AmazonDetectiveFullAccess a suas identidades do IAM.

Essa política concede permissões administrativas que permitem que a entidade principal tenha acesso total a todas as ações do Amazon Detective. É possível anexar essa política à entidade principal antes que o Detective seja habilitado na conta. Também deve ser anexado à função usada para executar os scripts do Python do Detective para criar e gerenciar um gráfico de comportamento.

As entidades principais com essas permissões podem gerenciar as contas-membro, adicionar tags ao gráfico de comportamento e usar o Detective para investigar. Eles também podem arquivar GuardDuty as descobertas. A política fornece as permissões que o console do Detective precisa para exibir os nomes das contas que estão inseridas. AWS Organizations

Detalhes de permissão

Esta política inclui as seguintes permissões:

- **detective**: permite acesso total das entidades principais a todas as ações do Detective.
- **organizations**: permite que as entidades principais recuperem do AWS Organizations informações sobre as contas em uma organização. Se uma conta pertencer a uma organização, essas permissões permitem que o console do Detective exiba os nomes das contas, além dos números das contas.
- **guardduty**— Permite que os diretores obtenham e arquivem GuardDuty as descobertas de dentro do Detective.
- **securityhub**: permite que as entidades principais obtenham as descobertas do Security Hub de dentro do Detective.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:*",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:ArchiveFindings"
      ],
      "Resource": "arn:aws:guardduty:*:*:detector/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
    }
  ]
}
```

```
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "securityHub:GetFindings"
        ],
        "Resource": "*"
    }
]
```

AWS política gerenciada: AmazonDetectiveMemberAccess

Também é possível anexar a política `AmazonDetectiveMemberAccess` às suas entidades do IAM.

Essa política fornece acesso de membro ao Amazon Detective e acesso limitado ao console.

Com essa política, você pode:

- Visualizar os convites de associação ao gráfico do Detective e aceitar ou rejeitar esses convites.
- Visualizar como sua atividade no Detective contribui para o custo de uso desse serviço na página [Uso](#).
- Renunciar de sua associação a um gráfico.

Esta política concede permissões somente leitura que oferecem acesso limitado ao console do Detective.

Detalhes de permissão

Esta política inclui as seguintes permissões:

- `detective`: permite que os membros acessem o Detective.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource": "*"
    }
  ]
}
```

Política gerenciada AWS : AmazonDetectiveInvestigatorAccess

Também é possível anexar a política `AmazonDetectiveInvestigatorAccess` às suas entidades do IAM.

Esta política fornece ao investigador acesso ao serviço do Detective e acesso limitado às dependências da interface do usuário do console do Detective. Esta política também concede aos usuários e perfis do IAM permissões para habilitar as investigações do Detective no Detective. Você pode realizar investigações para identificar indicadores de comprometimento, como descobertas, usando um relatório de investigação, que fornece análises e insights sobre indicadores de segurança. O relatório é classificado por gravidade, que é determinada usando a análise comportamental e o machine learning do Detective. Você pode usar o relatório para priorizar a correção de recursos.

Detalhes de permissão

Esta política inclui as seguintes permissões:

- **detective**: permite que as entidades principais tenham acesso de investigador às ações do Detective, habilitem as investigações do Detective e habilitem resumos de grupos de descobertas.
- **guardduty**— Permite que os diretores obtenham e arquivem GuardDuty as descobertas de dentro do Detective.
- **securityhub**: permite que as entidades principais obtenham as descobertas do Security Hub de dentro do Detective.
- **organizations**— permite que os diretores recuperem informações sobre as contas em uma organização de AWS Organizations. Se uma conta pertencer a uma organização, essas permissões permitem que o console do Detective exiba os nomes das contas, além dos números das contas.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DetectivePermissions",
      "Effect": "Allow",
      "Action": [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
        "detective:GetGraphIngestState",
        "detective:GetMembers",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListDatasourcePackages",
        "detective:ListGraphs",
        "detective:ListHighDegreeEntities",
        "detective:ListInvitations",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "detective:SearchGraph",
        "detective:StartInvestigation",
        "detective:GetInvestigation",
        "detective:ListInvestigations",
        "detective:UpdateInvestigationState",
        "detective:ListIndicators",
      ]
    }
  ]
}
```

```
    "detective:InvokeAssistant"
  ],
  "Resource": "*"
},
{
  "Sid": "OrganizationsPermissions",
  "Effect": "Allow",
  "Action": [
    "organizations:DescribeOrganization",
    "organizations:ListAccounts"
  ],
  "Resource": "*"
},
{
  "Sid": "GuardDutyPermissions",
  "Effect": "Allow",
  "Action": [
    "guardduty:ArchiveFindings",
    "guardduty:GetFindings",
    "guardduty:ListDetectors"
  ],
  "Resource": "*"
},
{
  "Sid": "SecurityHubPermissions",
  "Effect": "Allow",
  "Action": [
    "securityHub:GetFindings"
  ],
  "Resource": "*"
}
]
}
```

AWS política gerenciada: AmazonDetectiveOrganizationsAccess

Também é possível anexar a política AmazonDetectiveOrganizationsAccess às suas entidades do IAM.

Esta política concede permissão para habilitar e gerenciar o Amazon Detective dentro de uma organização. Você pode habilitar o Detective em toda a organização e determinar a conta de administrador delegado do Detective.

Detalhes de permissão

Esta política inclui as seguintes permissões:

- **detective**: permite que as entidades principais tenham acesso às ações do Detective.
- **iam**: especifica que uma função vinculada ao serviço é criada quando o Detective acionar `EnableOrganizationAdminAccount`.
- **organizations**— permite que os diretores recuperem informações sobre as contas em uma organização de AWS Organizations. Se uma conta pertencer a uma organização, essas permissões permitem que o console do Detective exiba os nomes das contas, além dos números das contas. Permite a integração de um AWS serviço, permite registrar e cancelar o registro da conta de membro especificada como administrador delegado e permite que os diretores recuperem contas de administrador delegado em outros serviços de segurança, como Amazon Detective, Amazon Macie e GuardDuty AWS Security Hub

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:DisableOrganizationAdminAccount",
        "detective:EnableOrganizationAdminAccount",
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "detective.amazonaws.com"
        }
      }
    }
  ],
}
```

```
{
  "Effect": "Allow",
  "Action": [
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "organizations:ServicePrincipal": [
        "detective.amazonaws.com"
      ]
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "organizations:ListDelegatedAdministrators"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "organizations:ServicePrincipal": [
        "detective.amazonaws.com",
        "guardduty.amazonaws.com",
        "macie.amazonaws.com",
        "securityhub.amazonaws.com"
      ]
    }
  }
}
]
```

```
}
```

AWS Política gerenciada da : AmazonDetectiveServiceLinkedRole

Não é possível anexar a política AmazonDetectiveServiceLinkedRole às suas entidades do IAM. Esta política é anexada a uma função vinculada ao serviço que permite que o Detective realize ações em seu nome. Para ter mais informações, consulte [the section called “Usar funções vinculadas a serviços”](#).

Esta política concede permissões administrativas que permitem que a função vinculada ao serviço recupere informações da conta em uma organização.

Detalhes de permissão

Esta política inclui as seguintes permissões:

- `organizations`: recupera as informações da conta de uma organização.

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

Detective atualizações em políticas gerenciadas AWS

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Detective desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações realizadas nesta página, assine o feed RSS na [página de histórico do documento do](#) .

Alteração	Descrição	Data
AmazonDetectiveInvestigatorAccess : atualizações em políticas existentes	<p>Foram adicionadas investigações do Detective e ações resumidas de grupos de descobertas à política <code>AmazonDetectiveInvestigatorAccess</code> .</p> <p>Essas ações permitem iniciar, recuperar e atualizar as investigações do Detective e obter um resumo de grupos de descobertas de dentro do Detective.</p>	26 de novembro de 2023
AmazonDetectiveFullAccess e AmazonDetectiveInvestigatorAccess : atualizações em políticas existentes	<p>O Detective adicionou ações <code>GetFindings</code> do Security Hub às políticas <code>AmazonDetectiveFullAccess</code> e <code>AmazonDetectiveInvestigatorAccess</code> .</p> <p>Essas ações permitem obter descobertas do Security Hub de dentro do Detective.</p>	16 de maio de 2023
AmazonDetectiveOrganizationsAccess – Nova política	<p>O Detective adicionou a política <code>AmazonDetectiveOrganizationsAccess</code> .</p> <p>Esta política concede permissão para habilitar e gerenciar o Detective dentro de uma organização</p>	2 de março de 2023
AmazonDetectiveMemberAccess – Nova política	<p>O Detective adicionou a política <code>AmazonDetectiveMemberAccess</code> .</p>	17 de janeiro de 2023

Alteração	Descrição	Data
	Esta política fornece acesso de membro ao Detective e acesso limitado à dependências da interface do usuário do console.	
AmazonDetectiveFullAccess : atualizações a uma política existente	<p>Detective adicionou GuardDuty GetFindings ações à política. AmazonDetectiveFullAccess</p> <p>Essas ações permitem obter GuardDuty descobertas de dentro do Detective.</p>	17 de janeiro de 2023
AmazonDetectiveInvestigatorAccess – Nova política	<p>O Detective adicionou a política AmazonDetectiveInvestigatorAccess .</p> <p>Esta política permite que a entidade principal conduza investigações no Detective.</p>	17 de janeiro de 2023
AmazonDetectiveServiceLinkedRole – Nova política	<p>O Detective adicionou uma nova política para sua função vinculada ao serviço.</p> <p>A política permite que a função vinculada ao serviço recupere informações sobre as contas na organização.</p>	16 de dezembro de 2021
O Detective começou a rastrear as alterações	Detective começou a monitorar as mudanças em suas políticas AWS gerenciadas.	10 de maio de 2021

Usar funções vinculadas ao serviço do Detective

O Amazon Detective usa funções vinculadas a [serviços AWS Identity and Access Management \(IAM\)](#). A função vinculada ao serviço é um tipo exclusivo de perfil do IAM vinculada diretamente ao Detective. As funções vinculadas ao serviço são predefinidas pelo Detective e incluem todas as permissões que o serviço exige para ligar para outros AWS serviços em seu nome.

Uma função vinculada a serviço facilita a configuração do Detective porque você não precisa adicionar as permissões necessárias manualmente. O Detective define as permissões das funções vinculadas ao serviço e, exceto se definido de outra forma, somente o Detective 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.

Um perfil vinculado ao serviço poderá ser excluído somente após excluir seus atributos relacionados. Isso protege seus recursos do Detective, pois você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros serviços que oferecem suporte às funções vinculadas a serviços, consulte [serviços da AWS compatíveis com o IAM](#) e procure os serviços que apresentam Sim na coluna Função vinculada a serviços. Escolha um Sim com um link para exibir a documentação da função vinculada a serviço desse serviço.

Permissões da função vinculada ao serviço do Detective

O Detective usa a função vinculada ao serviço chamada — `AWSServiceRoleForDetectivePermite` que o Detective acesse informações em seu nome. AWS Organizations

A função `AWSServiceRoleForDetective` vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `detective.amazonaws.com`

A função `AWSServiceRoleForDetective` vinculada ao serviço usa a política gerenciada.

[AmazonDetectiveServiceLinkedRolePolicy](#)

Para obter detalhes sobre as atualizações da `AmazonDetectiveServiceLinkedRolePolicy` política, consulte as [atualizações do Amazon Detective para políticas AWS gerenciadas](#). Para receber alertas automáticos sobre alterações nessa política, assine o feed RSS na página de histórico de [documentos do Detective](#).

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 obter mais informações, consulte [Permissões de função vinculada a serviços](#) no Guia do usuário do IAM.

Criar uma função vinculada ao serviço do Detective

Você não precisa criar manualmente uma função vinculada a serviço. Quando você designa a conta de administrador do Detective para uma organização na, na ou AWS Management Console na API, AWS CLI o Detective cria AWS a função vinculada ao serviço para você.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, você poderá usar esse mesmo processo para recriar o perfil em sua conta. Quando você designa a conta de administrador do Detective para uma organização, o Detective cria novamente a função vinculada ao serviço para você.

Editar uma função vinculada ao serviço do Detective

Detective não permite que você edite a função vinculada ao `AWSServiceRoleForDetective` 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 ter mais informações, consulte [Editar um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço do Detective

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

Note

Se o serviço do Detective 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 excluir os recursos do Detective usados pelo `AWSServiceRoleForDetective`

1. Remova a conta de administrador do Detective. Consulte [the section called “Designar a conta de administrador do Detective”](#).
2. Repita o processo em cada região em que você designou a conta de administrador do Detective.

Como excluir manualmente a função vinculada a serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função `AWSServiceRoleForDetective` vinculada ao serviço. Para mais informações, consulte [Excluir um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Regiões compatíveis com funções vinculadas ao serviço do Detective

O Detective oferece suporte a funções vinculadas ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte [Regiões e endpoints da AWS](#).

Solução de problemas de identidade e acesso do Amazon Detective

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o Detective e o IAM. Se você encontrar problemas de acesso negado ou dificuldades semelhantes ao trabalhar com o AWS Identity and Access Management(IAM), consulte os tópicos de [solução de problemas do IAM](#) no Guia do usuário do IAM.

Não tenho autorização para executar uma ação no Detective

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

O exemplo de erro a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para aceitar um convite para se tornar uma conta-membro de um gráfico de comportamento, mas não tem as permissões `detective:AcceptInvitation`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
perform: detective:AcceptInvitation on resource: arn:aws:detective:us-
east-1:444455556666:graph:567856785678
```

Neste caso, Mateo pede ao administrador para atualizar suas políticas para permitir a ele o acesso ao recurso `arn:aws:detective:us-east-1:444455556666:graph:567856785678` usando a ação `detective:AcceptInvitation`.

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, as suas políticas deverão ser atualizadas para permitir a passagem de um perfil para o Detective.

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 uma usuária do IAM chamada `marymajor` tenta usar o console para executar uma ação no Detective. 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 AWS conta acessem meus recursos de Detective

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

Para saber mais, consulte:

- Para saber se o Detective oferece suporte a esses recursos, consulte [Como o Amazon Detective 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.

Registro e monitoramento no Amazon Detective

O Amazon Detective é integrado. AWS CloudTrail CloudTrail captura todas as chamadas de API para Detective como eventos.

Para obter detalhes sobre como usar o CloudTrail registro para Detective, consulte. [the section called “Registrando chamadas da API Detective com CloudTrail”](#)

Validação de compatibilidade do Amazon Detective

O Amazon Detective está no escopo do programa de AWS garantia. Para obter mais informações, consulte a [Estrutura de Segurança Comum da Health Information Trust Alliance \(HITRUST\)](#).

Para obter uma lista de AWS serviços no escopo de programas de conformidade específicos, consulte [Serviços da AWS no escopo do programa de conformidade](#) . 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 [Fazer download de relatórios no AWS Artifact](#).

AWS fornece os seguintes recursos para ajudar na conformidade:

- [Guias de início rápido de segurança e compatibilidade](#): estes guias de implantação abordam as considerações de arquitetura e fornecem etapas para implantação de ambientes de linha de base focados em compatibilidade e segurança na AWS.

- [Avaliação de recursos com as regras](#) do Guia do AWS Config Desenvolvedor — O AWS Config serviço avalia se suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- [AWS Security Hub](#)— Esse AWS serviço fornece uma visão abrangente do seu estado de segurança interno, AWS que ajuda você a verificar sua conformidade com os padrões e as melhores práticas do setor de segurança.

Resiliência no Amazon Detective

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte [Infraestrutura AWS global](#).

Além da infraestrutura AWS global, o Detective usa a resiliência incorporada ao Amazon DynamoDB e ao Amazon Simple Storage Service (Amazon S3).

A arquitetura do Detective também é resistente às falhas de uma única zona de disponibilidade. Essa resiliência é incorporada ao Detective e não requer nenhuma configuração.

Segurança da infraestrutura no Amazon Detective

Como um serviço gerenciado, o Amazon Detective; 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 o Detective; por meio da 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 você pode usar o [AWS Security Token Service](#) (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Práticas recomendadas de segurança para o Amazon Detective

O Detective oferece uma série de recursos de segurança a serem considerados no desenvolvimento e na implementação das 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.

Para o Detective, as melhores práticas de segurança estão associadas ao gerenciamento das contas em um gráfico de comportamento.

Melhores práticas para contas de administradores

Ao convidar contas-membro para seu gráfico de comportamento, convide somente contas que você supervisiona.

Limite o acesso ao gráfico de comportamento. Quando um usuário tem acesso a um gráfico de comportamento, ele pode ver todas as descobertas das contas-membro. Essas descobertas podem expor informações confidenciais de segurança.

Práticas recomendadas para contas-membro

Ao receber um convite para um gráfico de comportamento, certifique-se de validar a origem do convite.

Verifique o identificador da AWS conta do administrador que enviou o convite. Verifique se você sabe a quem pertence a conta e se a conta que fez o convite tem um motivo legítimo para monitorar seus dados de segurança.

Previsão e monitoramento dos custos do Amazon Detective

Para ajudar você a monitorar sua atividade no Detective, a página Uso mostra a quantidade de dados ingeridos e o custo projetado.

- Para contas de administrador, a página Uso mostra o volume de dados e o custo projetado em todo o gráfico de comportamento.
- Para contas-membro, a página Uso mostra o volume de dados e o custo projetado de suas contas nos gráficos de comportamento para os quais elas contribuem.

Detective também oferece suporte AWS CloudTrail ao registro.

Conteúdo

- [Sobre a avaliação gratuita de gráficos de comportamento](#)
- [Monitorar o uso e o custo de um gráfico de comportamento \(conta de administrador\)](#)
- [Monitorar o uso e o custo em gráficos de comportamento \(conta-membro\)](#)
- [Como o Amazon Detective calcula o custo projetado](#)
- [Registro de chamadas da API Amazon Detective com AWS CloudTrail](#)

Sobre a avaliação gratuita de gráficos de comportamento

O Amazon Detective oferece uma avaliação gratuita de 30 dias para cada conta em cada região. A avaliação gratuita de uma conta começa na primeira vez em que ocorre uma das seguintes ações.

- Uma conta habilita o Detective manualmente e se torna a conta de administrador de um gráfico de comportamento.
- Uma conta é designada como a conta de administrador do Detective para uma organização no AWS Organizations e o Detective é habilitado pela primeira vez.
- Se a conta de administrador do Detective já tinha o Detective habilitado antes de ser designada, a conta não iniciará uma nova avaliação gratuita de 30 dias.
- Uma conta aceita um convite para ser uma conta-membro em um gráfico de comportamento e é habilitada como conta-membro.
- Uma conta da organização é habilitada como conta-membro pela conta de administrador do Detective.

A avaliação gratuita dura 30 dias a partir desse momento. A conta não é cobrada por nenhum dado processado durante esse período. Quando o período de avaliação termina, o Detective começa a cobrar a conta pelos dados que ela contribui nos gráficos de comportamento. Para obter mais informações sobre como você pode rastrear sua atividade no Detective, monitorar o uso e visualizar o custo projetado, consulte [Previsão e monitoramento dos custos do Amazon Detective](#). Para obter mais informações sobre a definição de preço, consulte [Definição de preço do Detective](#).

O mesmo período de 30 dias é usado para todos os gráficos de comportamento na região. Por exemplo, uma conta é habilitada como conta-membro em um gráfico de comportamento. Isso inicia a avaliação gratuita de 30 dias. Após 10 dias, a conta é habilitada para um segundo gráfico de comportamento na mesma região. Para o segundo gráfico de comportamento, a conta recebe 20 dias de dados gratuitos.

A avaliação gratuita oferece vários benefícios:

- As contas de administrador podem explorar os recursos e funcionalidades do Detective para verificar seu valor.
- As contas de administrador e contas-membro podem monitorar a quantidade de dados e o custo estimado antes que o Detective comece a cobrá-las. Consulte [the section called “Uso e custo de uma conta de administrador”](#) e [the section called “Rastreamento do uso da conta-membro”](#).

Avaliação gratuita para fontes de dados opcionais

O Detective também oferece uma avaliação gratuita de 30 dias para fontes de dados opcionais. Essa avaliação gratuita é separada daquela fornecida para as principais fontes de dados do Detective quando ele é habilitado pela primeira vez.

Note

Se um cliente desabilitar um pacote de fonte de dados opcional dentro de 7 dias após habilitá-lo, o Detective fará uma redefinição automática única da avaliação gratuita desse pacote de fonte de dados, caso ele seja habilitado novamente.

Para habilitar ou desabilitar um pacote de fonte de dados opcional, consulte [Tipos de fontes de dados principais no Detective](#).

Monitorar o uso e o custo de um gráfico de comportamento (conta de administrador)

O Amazon Detective cobra de cada conta os dados usados em cada gráfico de comportamento ao qual a conta pertence. O Detective cobra uma tarifa fixa nivelada por GB para todos os dados, independentemente da fonte.

Para contas de administrador, a página Uso do console do Detective permite que você visualize o volume de dados ingeridos Por fonte de dados ou Por conta nos últimos 30 dias. A conta de administrador também vê o custo projetado para um período típico de 30 dias para a conta e para todo o gráfico de comportamento.

Para ver as informações de uso do Detective

1. Faça login no AWS Management Console. Em seguida, abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, em Configurações, selecione Uso.
3. Escolha uma guia para selecionar entre visualizar o uso Por fonte de dados ou Por conta.

Volume de dados ingeridos para cada conta

Volume ingerido por conta-membro lista as contas ativas no gráfico de comportamento. As contas-membro que foram removidas não são listadas.

Para cada conta, a lista de volume ingerido fornece as seguintes informações.

- O identificador da AWS conta e o endereço de e-mail do usuário raiz.
- A data em que a conta começou a contribuir com dados no gráfico de comportamento.

Para a conta de administrador, essa é a data em que a conta habilitou o Detective.

Para contas-membro, essa é a data em que uma conta foi habilitada como conta-membro após aceitar o convite.

- O volume de dados ingeridos da conta nos últimos 30 dias. O total inclui todos os tipos de fonte.
- Se a conta está atualmente no período de avaliação gratuita. Para contas que estão atualmente em seu período de avaliação gratuita, a lista exibe o número de dias restantes.

Se nenhuma das contas estiver no período de avaliação gratuita, a coluna de status da avaliação gratuita não será exibida.

Custos projetados para o gráfico de comportamento

Custo projetado desta conta mostra o custo projetado para 30 dias de dados para a conta de administrador. O custo projetado é baseado no volume médio diário da conta de administrador.

Important

Esse valor é apenas um custo projetado. Ele projeta o custo total dos dados da conta de administrador para um período típico de 30 dias. É baseado no uso dos últimos 30 dias. Consulte [the section called “Como o Detective calcula o custo projetado”](#).

Custo projetado para o gráfico de comportamento

Custo projetado de todas as contas mostra o custo total projetado para 30 dias de dados para todo o gráfico de comportamento. O custo projetado é baseado no volume médio diário de cada conta.

Important

Esse valor é apenas um custo projetado. Ele projeta o custo total dos dados do gráfico de comportamento para um período típico de 30 dias. É baseado no uso dos últimos 30 dias. O custo projetado não inclui contas-membro que foram removidas do gráfico de comportamento. Consulte [the section called “Como o Detective calcula o custo projetado”](#).

Volume de dados ingeridos pelos pacotes de origem

Selecione Por pacote de origem para visualizar o volume de dados ingeridos listado pelos diferentes pacotes de origem habilitados no gráfico de comportamento.

Todas as contas podem visualizar esses dados para suas próprias contas. Uma conta de administrador pode ver painéis adicionais que listam o uso por pacote de origem para cada membro. As contas-membro que foram removidas não são listadas.

Painéis Principais do Detective

Os painéis principais do Detective mostram o volume de dados ingeridos das principais fontes do Detective (registros CloudTrail, registros de fluxo de VPC e GuardDuty descobertas) nos últimos 30 dias.

Logs de auditoria do EKS

Os painéis de Logs de auditoria do EKS mostram o volume de dados ingeridos das fontes de logs de auditoria do EKS nos últimos 30 dias. Os painéis desse pacote de origem só estarão disponíveis se os logs de auditoria do EKS estiverem habilitados no gráfico de comportamento.

Monitorar o uso e o custo em gráficos de comportamento (conta-membro)

O Amazon Detective cobra de cada conta os dados usados em cada gráfico de comportamento ao qual a conta pertence. O Detective cobra uma tarifa fixa nivelada por GB para todos os dados, independentemente da fonte.

Para contas-membro, a página Uso mostra o volume de dados e o custo projetado de 30 dias somente para essa conta.

Para ver as informações de uso do Detective

1. Faça login no AWS Management Console. Em seguida, abra o console do Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, em Configurações, selecione Uso.

Volume ingerido para cada gráfico de comportamento

Volume ingerido dessa conta lista os gráficos de comportamento para os quais a conta-membro contribui. Não inclui associações às quais você renunciou ou associações que a conta de administrador removeu.

Para cada gráfico de comportamento, a lista inclui as informações a seguir.

- O número de conta da conta de administrador
- O volume de dados ingeridos da conta-membro nos últimos 30 dias. O total inclui todos os tipos de fonte.

- A data em que a conta-membro foi habilitada no gráfico de comportamento.

Custo projetado em todos os gráficos de comportamento

Custo projetado dessa conta mostra um custo projetado para 30 dias de dados da conta-membro em todos os gráficos de comportamento para os quais ela contribui. O custo projetado é baseado no volume médio diário da conta-membro.

Important

Esse valor é apenas um custo projetado. Ele projeta o custo total dos dados da conta de administrador para um período típico de 30 dias. É baseado no uso dos últimos 30 dias. Consulte [the section called “Como o Detective calcula o custo projetado”](#).

Como o Amazon Detective calcula o custo projetado

Para calcular os valores do custo projetado que são exibidos na página Uso, o Detective faz o seguinte.

1. Para obter o custo projetado para uma conta individual em um gráfico de comportamento, o Detective faz o seguinte.
 - a. Calcula o volume médio por dia. Adiciona o volume de dados em todos os dias ativos e, depois, divide pelo número de dias em que a conta esteve ativa.

Se a conta foi habilitada há mais de 30 dias, o número de dias será 30. Se a conta foi habilitada há menos de 30 dias, o número será a quantidade de dias desde a data de aceite.

Por exemplo, se a conta foi habilitada há 12 dias, o Detective adiciona o volume ingerido nesses 12 dias e o divide por 12.
 - b. Multiplica a média diária da conta por 30. Esse é o uso projetado da conta para 30 dias.
 - c. Usa o modelo de definição de preço para calcular o custo projetado de 30 dias para o uso projetado de 30 dias.
2. Para obter o custo total projetado para um gráfico de comportamento, o Detective faz o seguinte:
 - a. Combina o uso projetado de 30 dias de todas as contas no gráfico de comportamento.
 - b. Usa o modelo de definição de preço para calcular o custo projetado de 30 dias para o uso total projetado de 30 dias.

3. Para obter o custo total projetado para uma conta-membro entre os gráficos de comportamento, o Detective faz o seguinte:
 - a. Combina o uso projetado de 30 dias de todos os gráficos de comportamento.
 - b. Usa o modelo de definição de preço para calcular o custo projetado de 30 dias para o uso total projetado de 30 dias.
4. Se você estiver usando um Amazon VPC compartilhado, o Detective calculará o custo projetado com base na atividade de monitoramento. Recomendamos revisar o custo projetado para suas investigações específicas do seu ambiente.
 - a. Se uma conta-membro do Detective tiver um Amazon VPC compartilhado e houver outras contas que não são do Detective usando a VPC compartilhada, o Detective monitorará todo o tráfego dessa VPC. O uso e o custo aumentarão e o Detective fornecerá visualização sobre todo o fluxo de tráfego dentro da VPC.
 - b. Se você tiver uma instância do EC2 dentro de um Amazon VPC compartilhado e o proprietário compartilhado não for membro do Detective, o Detective não monitorará nenhum tráfego da VPC e o uso e o custo diminuirão. Se você quiser visualizar o fluxo de tráfego dentro da VPC, deverá adicionar o proprietário do Amazon VPC como membro do seu gráfico do Detective.

Registro de chamadas da API Amazon Detective com AWS CloudTrail

Detective é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Detective. CloudTrail captura todas as chamadas de API para Detective como eventos. As chamadas capturadas incluem as chamadas do console do Detective e as chamadas de código para as operações da API do Detective.

- Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para Detective.
- Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos.

Usando as informações coletadas por CloudTrail, você pode determinar o seguinte:

- A solicitação feita ao Detective
- O endereço IP do qual a solicitação foi feita.

- Quem fez a solicitação.
- Quando ela foi feita
- Detalhes adicionais sobre a solicitação

Para saber mais sobre isso CloudTrail, consulte o [Guia AWS CloudTrail do usuário](#).

Informações de Detective em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando a atividade ocorre no Detective, essa atividade é registrada em um CloudTrail evento, junto com outros eventos de AWS serviço, no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua conta da AWS . Para obter mais informações, consulte [Visualização de eventos com histórico de CloudTrail eventos](#).

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos para Detective, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3.

Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS . A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Você também pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros.

Para mais informações, consulte:

- [Visão Geral para Criar uma Trilha](#)
- [CloudTrail Serviços e integrações compatíveis](#)
- [Configurando notificações do Amazon SNS para CloudTrail](#)
- [Recebendo arquivos de CloudTrail log de várias regiões](#) e [recebendo arquivos de CloudTrail log de várias contas](#)

CloudTrail registra todas as operações do Detective, que estão documentadas na Referência da API [Detective](#).

Por exemplo, chamadas para as `DeleteMembers` operações `CreateMembersAcceptInvitation`, e geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM)
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado
- Se a solicitação foi feita por outro AWS serviço

Para obter mais informações, consulte o elemento [CloudTrail UserIdentity](#).

Noções básicas sobre entradas de arquivos de log do Detective

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log.

Um evento representa uma solicitação única de qualquer fonte. Os eventos incluem informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, as entradas não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `AcceptInvitation` ação.

```
{
  "EventId": "f2545ee3-170f-4340-8af4-a983c669ce37",
  "Username": "JaneRoe",
  "EventTime": 1571956406.0,
  "CloudTrailEvent": "{\"eventVersion\":\"1.05\",\"userIdentity\":{
    \"type\":\"AssumedRole\",\"principalId\":\"AR0AJZARKEP6WKJ5JHSUS:JaneRoe\",
    \"arn\":\"arn:aws:sts::111122223333:assumed-role/1A4R5SKSPGG9V/JaneRoe\",
    \"accountId\":\"111122223333\",
    \"accessKeyId\":\"AKIAIOSFODNN7EXAMPLE\",
    \"sessionContext\":{
      \"attributes\":{\"mfaAuthenticated\":\"false\"},
      \"creationDate\":\"2019-10-24T21:54:56Z\",
      \"sessionIssuer\":{\"type\":\"Role\",\"principalId\":\"AR0AJZARKEP6WKJ5JHSUS\",
        \"arn\":\"arn:aws:iam::111122223333:role/1A4R5SKSPGG9V\",
        \"accountId\":\"111122223333\",
        \"userName\":\"JaneRoe\"}}},
    \"eventTime\":\"2019-10-24T22:33:26Z\",
    \"eventSource\":\"detective.amazonaws.com\",
    \"eventName\":\"AcceptInvitation\",
    \"awsRegion\":\"us-east-2\",
    \"sourceIPAddress\":\"192.0.2.123\",
    \"userAgent\":\"aws /3 aws-sdk-java/1.11.648 Linux/4.14.133-97.112.amzn2.x86_64 OpenJDK_64-Bit_Server_VM/25.201-b09 java/1.8.0_201 vendor/Oracle_Corporation exec-env/AWS_Lambda_java8\",
    \"errorCode\":\"ValidationException\",
    \"requestParameters\":
```

```
{\"masterAccount\": \"111111111111\"}, \"responseElements\": {\"message\": \"Invalid request body\"}, \"requestID\": \"8437ff99-5ec4-4b1a-8353-173be984301f\", \"eventID\": \"f2545ee3-170f-4340-8af4-a983c669ce37\", \"readOnly\": false, \"eventType\": \"AwsApiCall\", \"recipientAccountId\": \"11112223333\"},  
  \"EventName\": \"AcceptInvitation\",  
  \"EventSource\": \"detective.amazonaws.com\",  
  \"Resources\": []  
},
```

Regiões e cotas do Amazon Detective

Ao usar o Amazon Detective, preste atenção a essas cotas.

Regiões e endpoints do Detective

Para ver a lista de Regiões da AWS onde o Detective está disponível, consulte Pontos finais do serviço de [detective](#).

Cotas do Detective

O Detective tem as seguintes cotas, que não podem ser configuradas.

Recurso	Cota	Comentários
Número de contas-membro	1.200	O número de contas-membro que uma conta de administrador pode adicionar a um gráfico de comportamento.
Volume de dados do gráfico de comportamento — aviso de volume	9 TB por dia	Se o volume de dados do gráfico de comportamento for maior que 9 TB por dia, o Detective exibirá um aviso de que o gráfico de comportamento está próximo do volume máximo permitido.
Volume de dados do gráfico de comportamento — sem novas contas	10 TB por dia	Se o volume de dados do gráfico de comportamento for maior que 10 TB por dia, você não poderá adicionar novas contas-membro ao gráfico de comportamento.
Volume de dados do gráfico de comportamento — interrupção da ingestão de dados no gráfico de comportamento	15 TB por dia	Se o volume de dados do gráfico de comportamento for maior que 15 TB por dia, o Detective interrompe a ingestão de dados no gráfico de comportamento.

Recurso	Cota	Comentários
		<p>Os 15 TB por dia refletem tanto o volume de dados normal quanto os picos no volume de dados.</p> <p>Para reabilitar a ingestão de dados, você deve entrar em contato com o AWS Support.</p>

Internet Explorer 11 não compatível

Você não pode usar o Detective no Internet Explorer 11.

Gerenciar tags em um gráfico de comportamento

Você pode atribuir tags ao seu gráfico de comportamento. Em seguida, você pode usar os valores das tags nas políticas do IAM para gerenciar o acesso às funções do gráfico de comportamento no Detective. Consulte [the section called “Autorização baseada em tags dos gráficos de comportamento do Detective”](#).

Você também pode usar as tags como uma ferramenta para relatórios de custos. Por exemplo, para monitorar os custos associados à segurança, você pode atribuir a mesma tag ao gráfico de comportamento do Detective, ao recurso do AWS Security Hub hub e aos detectores da Amazon GuardDuty . Em seguida AWS Cost Explorer, você pode pesquisar essa tag para ter uma visão consolidada dos custos desses recursos.

Visualizar as tags de um gráfico de comportamento (console)

Você pode gerenciar as tags de um gráfico de comportamento na página Geral.

Para visualizar a lista de tags atribuídas ao gráfico de comportamento

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação, em Configurações, selecione Geral.

Listar as tags de um gráfico de comportamento (API do Detective, AWS CLI)

Você pode usar a Detective API ou a AWS Command Line Interface para obter a lista de tags para seu gráfico de comportamento.

Para obter a lista de tags para um gráfico de comportamento (Detective API,) AWS CLI

- API do Detective: use a operação [ListTagsForResource](#). Você deve fornecer o ARN do gráfico de comportamento.
- AWS CLI: na linha de comando, execute o comando `list-tags-for-resource`.

```
aws detective list-tags-for-resource --resource-arn <behavior graph ARN>
```

Exemplo

```
aws detective list-tags-for-resource --resource-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Adicionar tags a um gráfico de comportamento (console)

Na lista de tags na página Geral, você pode adicionar valores de tags ao gráfico de comportamento.

Para adicionar uma tag ao gráfico de comportamento

1. Selecione Adicionar nova tag.
2. Em Chave, insira o nome da tag.
3. Em Valor, insira o valor da tag.

Adicionar tags a um gráfico de comportamento (Detective API,) AWS CLI

Você pode usar a Detective API ou a AWS CLI para adicionar valores de tag ao seu gráfico de comportamento.

Para adicionar tags a um gráfico de comportamento (Detective API,) AWS CLI

- API do Detective: use a operação [TagResource](#). Você fornece o ARN do gráfico de comportamento e os valores de tags a serem adicionados.
- AWS CLI: na linha de comando, execute o comando `tag-resource`.

```
aws-detective tag-resource --aws detective tag-resource --resource-arn <behavior graph ARN> --tags '{"TagName":"TagValue"}
```

Exemplo

```
aws detective tag-resource --resource-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234 --tags '{"Department":"Finance"}
```

Remover tags de um gráfico de comportamento (console)

Para remover uma tag da lista na página Geral, escolha a opção Remover para essa tag.

Remover tags de um gráfico de comportamento (API do Detective, AWS CLI)

Você pode usar a Detective API ou a AWS CLI para remover os valores das tags do seu gráfico de comportamento.

Para remover tags de um gráfico de comportamento (Detective API,) AWS CLI

- API do Detective: use a operação [UntagResource](#). Você fornece o ARN do gráfico de comportamento e os nomes das tags a serem removidas.
- AWS CLI: na linha de comando, execute o comando `untag-resource`.

```
aws detective untag-resource --resource-arn <behavior graph ARN> --tag-keys "TagName"
```

Exemplo

```
aws detective untag-resource --resource-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234 --tag-keys "Department"
```


Desabilitar o Amazon Detective

A conta de administrador de um gráfico de comportamento pode desabilitar o Amazon Detective no console do Detective, na API do Detective ou no AWS Command Line Interface. Ao desabilitar o Detective, o gráfico de comportamento e os dados associados ao Detective são excluídos.

Depois que um gráfico de comportamento é excluído, não pode ser restaurado.

Conteúdo

- [Desabilitar o Detective \(Console\)](#)
- [Desativando o Detective \(Detective API,\) AWS CLI](#)
- [Desativando o Detective em todas as regiões \(script Python ativado\) GitHub](#)

Desabilitar o Detective (Console)

Você pode desabilitar o Amazon Detective no AWS Management Console.

Para desativar o Amazon Detective (console)

1. Abra o console do Amazon Detective em <https://console.aws.amazon.com/detective/>.
2. No painel de navegação do Detective, em Configurações, selecione Geral.
3. Na página Geral, em Desativar o Amazon Detective, escolha Desativar o Amazon Detective.
4. Quando for solicitado, digite **disable** para confirmar.
5. Escolha Desativar Amazon Detective.

Desativando o Detective (Detective API,) AWS CLI

Você pode desabilitar o Amazon Detective na API do Detective ou no AWS Command Line Interface. Para obter o ARN do gráfico de comportamento para usar na solicitação, use a operação [ListGraphs](#).

Para desativar o Detective (Detective API,) AWS CLI

- API do Detective: use a operação [DeleteGraph](#). Você deve fornecer o ARN do gráfico.
- AWS CLI: na linha de comando, execute o comando [delete-graph](#).

```
aws detective delete-graph --graph-arn <graph ARN>
```

Exemplo:

```
aws detective delete-graph --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Desativando o Detective em todas as regiões (script Python ativado) GitHub

Detective fornece um script de código aberto GitHub que permite desativar o Detective para uma conta de administrador em uma lista específica de regiões.

Para obter informações sobre como configurar e usar os GitHub scripts, consulte [the section called “Scripts em Python do Amazon Detective”](#).

Histórico do documento do Guia do usuário do Detective

A tabela a seguir descreve as alterações importantes na documentação desde a última versão do Detective. Para receber notificações sobre atualizações dessa documentação, você poderá se inscrever em um feed RSS.

- Última atualização da documentação: 15 de maio de 2024

Alteração	Descrição	Data
Novas versões de origem do Security Lake	Além da versão de origem 1 (OCSF 1.0.0-rc.2), o Detective agora ingere dados da versão 2 (OCSF 1.1.0) para as fontes do Security Lake que são suportadas pelo Detective.	15 de maio de 2024
Nova fonte de log do Security Lake	Você pode usar a integração do Detective com o Security Lake para coletar registros e eventos dos registros de auditoria do Amazon EKS .	15 de maio de 2024
Atualização da documentação	O conteúdo do Amazon Detective Administration Guide agora está consolidado no Amazon Detective User Guide. O Amazon Detective Administration Guide chegará ao fim do suporte padrão em 08 de maio de 2024.	15 de abril de 2024
Suporte adicional para GuardDuty descobertas da Amazon	O Detective agora fornece suporte para os seguintes tipos de descoberta do GuardDuty Runtime Monitoring . Execution:Runtime/	5 de abril de 2024

MaliciousFileExecu
ted Execution
:Runtime/Suspiciou
sTool DefenseEv
asion:Runtime/
PtraceAntiDeb
ugging Execution
:Runtime/Suspiciou
sCommand DefenseEv
asion:Runtime/Susp
iciousCommand

[Removido o requisito de
GuardDuty associação à
Amazon](#)

Você não precisa mais ser
GuardDuty cliente para
habilitar o Amazon Detective.
O requisito de ter GuardDuty
ativado sua conta por 48 horas
antes de ativar o Detective foi
removido.

2 de fevereiro de 2022

[Suporte adicional para
GuardDuty descobertas da
Amazon](#)

Detective estende o suporte
aos tipos de descoberta do
[GuardDuty EC2 Runtime
Monitoring](#) aos recursos do
ECS e do EC2.

30 de janeiro de 2024

Funcionalidade atualizada

Agora você pode executar uma investigação de Detective na página Investigações de um recurso específico que você deseja investigar. O Detective recomenda recursos com base em sua atividade de descobertas e grupos de descobertas.

Detective Investigations

permite investigar usuários e funções do IAM com indicadores de comprometimento, o que pode ajudar a determinar se um recurso está envolvido em um incidente de segurança .

16 de janeiro de 2024

Funcionalidade atualizada

Agora você pode realizar uma investigação do Detective em um recurso recomendado na página Investigações. O Detective recomenda recursos com base em sua atividade de descobertas e grupos de descobertas.

Detective Investigations

permite investigar usuários e funções do IAM com indicadores de comprometimento, o que pode ajudar a determinar se um recurso está envolvido em um incidente de segurança .

26 de dezembro de 2023

[Alterações na forma como o Detective lê o tráfego de fluxo de VPCs compartilhadas](#)

Se você estiver usando um Amazon VPC compartilhado, poderá ver alterações no tráfego monitorado pelo Detective. Recomendamos que você analise as alterações em [Detalhes da atividade do volume total do fluxo da VPC](#) para compreender os possíveis efeitos em sua cobertura e analise [como o Detective calcula o custo projetado](#) para entender como isso pode afetar os custos de serviço.

20 de dezembro de 2023

[Disponibilidade regional](#)

Foram adicionadas as regiões Europa (Estocolmo), Europa (Paris) e Canadá (Central) à lista de AWS regiões em que a [integração do Detective com o Security Lake está disponível](#).

8 de dezembro de 2023

[Novo atributo](#)

As [investigações do Detective](#) permitem que você investigue usuários e perfis do IAM com indicadores de comprometimento, que podem ajudar você a determinar se um recurso está envolvido em um incidente de segurança.

26 de novembro de 2023

[Novo recurso](#)

Por padrão, o Detective automaticamente gera [resumos de grupos de descobertas](#) para grupos de descoberta, agora com tecnologia de inteligência artificial generativa (IA generativa). O resumo de grupo de descobertas rapidamente analisa as relações entre as descobertas e os recursos afetados e resume as possíveis ameaças em linguagem natural.

26 de novembro de 2023

[Novo recurso](#)

A [integração do Detective ao Security Lake](#) permite a consulta e recuperação dos dados de log bruto armazenados pelo Security Lake. Usando essa integração, você pode coletar registros e eventos de eventos de CloudTrail gerenciamento e registros de fluxo da Amazon Virtual Private Cloud (Amazon VPC).

26 de novembro de 2023

[Informações de políticas gerenciadas adicionadas ao capítulo sobre segurança](#)

Foram adicionadas investigações do Detective e ações resumidas de grupos de descobertas à política do AmazonDetectiveInvestigatorAccess .

26 de novembro de 2023

Visualizar a visão geral de uma descoberta	Se uma descoberta estiver relacionada a uma atividade maior, agora o Detective notifica você a ir para o grupo de descobertas.	18 de setembro de 2023
Endpoints e cotas do Amazon Detective	Agora o Detective está disponível na região de Israel (Tel Aviv).	25 de agosto de 2023
Visualização aprimorada dos grupos de descobertas	A visualização do resumo de grupos de descobertas do Detective agora inclui grupos com descobertas agregadas, tornando a análise de evidências, entidades e descobertas relacionadas mais eficiente.	8 de agosto de 2023
Aprimoramento dos grupos de descobertas	Os grupos de descobertas agora incluem descobertas de vulnerabilidades do Amazon Inspector.	13 de junho de 2023
Suporte adicional para o Amazon GuardDuty Lambda Protection	Detective agora fornece suporte para a Proteção Lambda GuardDuty .	26 de maio de 2023
Foram adicionadas descobertas de AWS segurança como um novo pacote opcional de fonte de dados.	Detective agora fornece descobertas AWS de segurança como um pacote de fonte de dados opcional. Esse pacote de fonte de dados opcional permite que o Detective consuma dados do Security Hub e os adicione ao gráfico de comportamento.	16 de maio de 2023

Suporte adicional para tipos de descoberta do Amazon GuardDuty EKS Runtime Monitoring	O Detective agora fornece suporte para GuardDuty os tipos de descoberta do EKS Runtime Monitoring.	3 de maio de 2023
Suporte adicional para tipos de descoberta do Amazon GuardDuty RDS Protection	Detective agora fornece suporte para tipos de descoberta do GuardDuty RDS Protection.	20 de abril de 2023
Suporte adicional para outros tipos de GuardDuty busca da Amazon	Detective agora fornece perfis para os seguintes tipos de GuardDuty descoberta adicionais: DefenseEvasion: EC2UnusualDNSResolver DefenseEvasion: EvasionEC2UnusualDoHActivity DefenseEvasion: EvasionEC2UnusualDoTActivity	12 de abril de 2023
Foram adicionados novos painéis no console do Detective para ajudar os usuários a selecionar a política gerenciada pela AWS adequada para seu caso de uso específico.	O Detective oferece políticas gerenciadas para escolher com segurança as permissões de que você precisa.	3 de abril de 2023
Exibir o tráfego de fluxo do VPC para clusters do EKS	Adicionada nova seção para o tráfego de fluxo da Amazon Virtual Private Cloud (Amazon VPC) com clusters do Amazon Elastic Kubernetes Service (Amazon EKS).	2 de março de 2023

[Grupos de descobertas agora incluem uma representação visual dinâmica do gráfico de comportamento do Detective](#)

Agora os grupos de descobertas do Detective incluem uma representação visual dinâmica do gráfico de comportamento do Detective para enfatizar o relacionamento entre entidades e descobertas dentro do grupo de descobertas.

28 de fevereiro de 2023

[Exportar dados da página Resumo do Detective e da página de resultados de pesquisa. Os dados são exportados no formato CSV \(valores separados por vírgula\).](#)

Agora o Detective oferece a opção de exportar dados para o seu navegador a partir do console do Detective.

7 de fevereiro de 2023

[Adicionado volume geral de fluxo do VPC para workloads EKS do Amazon EKS](#)

Agora o Detective adiciona resumos visuais e análises sobre seus logs de fluxo da nuvem privada virtual (VPC) da Amazon a partir de workloads do Amazon Elastic Kubernetes Service Amazon EKS.

19 de janeiro de 2023

Informações de políticas gerenciadas adicionadas ao capítulo sobre segurança	Detective agora apoia ações de GuardDuty obtenção de descobertas por meio da AmazonDetectiveFullAccess política. O capítulo de segurança agora fornece detalhes sobre as seguintes novas políticas gerenciadas para Detective: e. AmazonDetectiveMemberAccess AmazonDetectiveInvestigator Access	17 de janeiro de 2023
Retenção de dados adicionada	Com o Detective, você pode acessar até um ano de dados do histórico de eventos.	20 de dezembro de 2022
Adicionada a opção de ajustar o escopo de tempo na página de resumo.	Agora o Detective oferece a opção de ajustar o escopo de tempo para visualizar a atividade em qualquer período de 24 horas nos últimos 365 dias.	5 de outubro de 2022
Procurar uma descoberta ou entidade	Agora o Detective fornece pesquisa sem distinção entre maiúsculas e minúsculas.	3 de outubro de 2022
Adicionada a capacidade de definir o timestamp do escopo	Agora o Detective fornece uma forma de configurar a preferência de formato do timestamp do escopo. Essa preferência será aplicada a todos os timestamps no Detective.	3 de outubro de 2022

[Termos adicionados relacionados a grupos de descobertas](#)

Agora o Detective oferece suporte a grupos de descobertas que conectam descobertas relacionadas em uma única tela para ajudá-lo a investigar possíveis atividades maliciosas em seu ambiente. A partir de um perfil de grupo de descobertas, você pode ir aos perfis de entidades e às visões gerais das descobertas relacionadas a esse grupo.

3 de agosto de 2022

[Adicionados novos perfis associados aos logs de auditoria do Amazon EKS](#)

Agora o Detective fornece perfis para permitir que você investigue atividades associadas às seguintes entidades relacionadas a contêineres: clusters do Amazon EKS, imagens de contêineres, pods do Kubernetes e sujeitos do Kubernetes.

26 de julho de 2022

[Nova fonte de dados opcional adicionada](#)

O Detective agora oferece suporte aos logs de auditoria do EKS como um pacote de fonte de dados opcional. Uma conta de administrador pode habilitar essa nova fonte de dados em um gráfico de comportamento existente . Os gráficos criados após essa data terão essa fonte de dados habilitada por padrão. Os administradores podem desabilitar essa fonte de dados manualmente a qualquer momento.

26 de julho de 2022

[Nova função vinculada ao serviço e política gerenciada do Detective](#)

Agora o Detective tem uma função vinculada ao serviço, `AWSServiceRoleForDetective` . A função vinculada ao serviço é usada para acessar os dados do Organizations em seu nome. A função usa uma nova política gerenciada `AmazonDetectiveServiceLinkRolePolicy` .

16 de dezembro de 2021

[Integração adicional com AWS Organizations](#)

Agora o Detective está integrado ao Organizations. A conta de gerenciamento da organização designa uma conta de administrador do Detective para a organização. A conta de administrador do Detective pode visualizar todas as contas na organização e habilitá-las como contas-membro no gráfico de comportamento da organização.

16 de dezembro de 2021

[Perfis de descobertas substituídos por visões gerais de descobertas](#)

Os perfis de descobertas continham visualizações que analisavam a atividade do recurso envolvido. A nova visão geral da descoberta contém detalhes da descoberta ingeridos GuardDuty e uma lista das entidades envolvidas. Na visão geral de uma descoberta, você pode acessar os perfis das entidades relacionadas.

20 de setembro de 2021

[Removido o limite de tipos de GuardDuty descoberta compatíveis](#)

Detective não está mais limitado a um conjunto selecionado de tipos de GuardDuty descoberta. O Detective coleta automaticamente os detalhes da descoberta para todos os tipos de descoberta e fornece acesso aos perfis das entidades relacionadas.

20 de setembro de 2021

[Link para os detalhes da descoberta no painel de perfil da descoberta associada](#)

No perfil de uma entidade, ao escolher uma descoberta na lista de descobertas associadas, os detalhes da descoberta são exibidos no painel à direita. O escopo de tempo é definido como a janela de tempo da descoberta.

20 de setembro de 2021

[Adicionados buckets do S3 aos tipos de entidade disponíveis no Detective](#)

Agora o Detective fornece perfis para buckets do S3. Os perfis de buckets do S3 fornecem detalhes sobre as entidades principais que interagiram com o bucket do S3 e as operações de API que executaram no bucket do S3.

20 de setembro de 2021

[Nova opção para gerar URLs do Detective no Splunk](#)

O projeto Splunk Trumpet permite que você envie AWS conteúdo para o Splunk. O projeto agora permite que você adicione URLs de Detective para navegar até os perfis e obter descobertas. GuardDuty

8 de setembro de 2021

[AKIDs substituídos nos detalhes da atividade de contas e funções](#)

Nos perfis de conta, os detalhes da atividade do Volume geral de chamadas de API agora mostram usuários ou funções em vez de identificadores de chave de acesso (AKIDs). Nos perfis de função, os detalhes da atividade do Volume geral de chamadas de API agora mostram sessões de função em vez de AKIDs. Para atividades que ocorreram antes dessa alteração, o chamador é listado como Recurso desconhecido.

14 de julho de 2021

[Adicionado o serviço de chamadas às informações sobre chamadas de API](#)

No console do Detective, as informações sobre chamadas de API agora incluem o serviço que emitiu a chamada. Adicionada uma coluna de Serviço às listas de Volume geral de chamadas de API, Chamadas de API recém-observadas e Chamadas de API com aumento de volume. Nos detalhes da atividade do Volume geral de chamadas de API e das Geolocalizações recém-observadas, os métodos da API são agrupados nos serviços que os emitiram. Para atividades que ocorreram antes dessa alteração, os métodos da API são agrupados em Serviço desconhecido.

14 de julho de 2021

[Nova guia de Interação de recursos para usuários, funções e sessões de função](#)

A guia Interação de recursos para usuários, funções e sessões de função contém informações sobre a atividade de suposição de função que envolveu essas entidades . Para sessões de função, essa é uma nova guia. Para usuários e funções, essa é uma guia existente com novo conteúdo.

29 de junho de 2021

[Valores atualizados para cotas de volume de dados do gráfico de comportamento](#)

Aumentamos as cotas de volume de dados dos gráficos de comportamento. Com 3,24 TB por dia, o Detective emite um aviso. Com 3,6 TB por dia, nenhuma nova conta pode ser adicionada. Com 4,5 TB por dia, o Detective para a ingestão de dados no gráfico de comportamento.

10 de junho de 2021

[Valores de tag adicionados às opções de script do Python](#)

Ao usar o script `enableDetective.py` do Python para habilitar o Detective, você poderá atribuir valores de tag ao gráfico de comportamento.

19 de maio de 2021

[Habilitação automática adicionada para contas-membro que passam na verificação do volume de dados](#)

Quando as contas-membro aceitam um convite, seu status é Aceito (Não habilitado) até que o Detective verifique se seus dados não farão com que o volume de dados no gráfico de comportamento exceda a cota. Se o volume de dados não for um problema, o Detective alterará automaticamente o status para Aceito (Habilitado). Observe que as contas-membro existentes com status atual Aceito (Não habilitado) não podem ser habilitadas automaticamente.

12 de maio de 2021

[Informações de políticas gerenciadas adicionadas ao capítulo sobre segurança](#)

Uma nova seção no capítulo sobre segurança fornece os detalhes das políticas gerenciadas do Detective . Atualmente, o Detective fornece uma única política gerenciada, AmazonDetectiveFullAccess .

10 de maio de 2021

[Os valores do volume de dados na lista de contas-membro foram alterados](#)

Na página Gerenciamento de contas, agora a lista de contas-membro exibe o volume diário de dados de cada conta-membro. Anteriormente, a lista exibia o volume como uma porcentagem do volume total permitido.

29 de abril de 2021

[As opções para o gerenciamento de contas-membro foram revisadas](#)

Substituímos o menu Gerenciar contas por um menu de Ações. Combinamos as opções para adicionar contas individuais e contas de um arquivo .csv. Movemos a opção Habilitar contas de Gerenciar contas para uma opção separada ao lado de Ações.

5 de abril de 2021

[Tags de gráficos de comportamento e autorização com base em tags foram adicionadas](#)

Ao habilitar o Detective, você pode adicionar tags ao gráfico de comportamento. Você pode gerenciar as tags de um gráfico de comportamento na página Geral. O Detective também oferece suporte à autorização com base nos valores de tags.

31 de março de 2021

[Suporte adicional para outros tipos de GuardDuty busca da Amazon](#)

Detective agora fornece perfis para os seguintes tipos de GuardDuty descobertos adicionais: CredentialAccess: IAMUser/AnomalousBehavior, DefenseEvasion: IAMUser/AnomalousBehavior, Discovery: IAMUser/AnomalousBehavior, Exfiltration: IAMUser/AnomalousBehavior, Impact: IAMUser/AnomalousBehavior, InitialAccess: IAMUser/AnomalousBehavior, Persistence: IAMUser/AnomalousBehavior, PrivilegeEscalation: IAMUser/AnomalousBehavior

29 de março de 2021

[Diferenças adicionadas para AWS GovCloud \(US\) regiões](#)

Detective agora está disponível nas Regiões. AWS GovCloud (US) Em AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA), o Detective não envia e-mails de convite para as contas dos membros. O Detective também não remove automaticamente as contas-membro que estão encerradas na AWS.

24 de março de 2021

[Foram adicionadas guias para filtrar a lista de contas-membro com base no status da conta-membro](#)

Agora a lista de contas-membro exibe guias que você pode usar para filtrar a lista com base no status da conta-membro. Você pode visualizar todas as contas-membro, aquelas com o status Aceito (Habilitado) ou aquelas com o status diferente de Aceito (Habilitado).

16 de março de 2021

[Suporte adicional para outros tipos de GuardDuty busca da Amazon](#)

Detective agora fornece perfis para os seguintes tipos de GuardDuty descoberta adicionais: Backdoor:EC2/C&CActivity.B,,Impact:EC2/PortSweep ,e Impact:EC2/WinRMBruteForcePrivilegeEscalation:IAMUser/AdministrativePermissions

4 de março de 2021

A opção de script do Python para suprimir e-mails de convite foi adicionada	Agora o script <code>enableDetective.py</code> do Detective oferece a opção <code>--disable_email</code> . Ao incluir essa opção, o Detective não envia e-mails de convite para as contas-membro.	26 de fevereiro de 2021
“Conta principal” é alterado para “conta de administrador”	O termo “conta principal” é alterado para “conta de administrador”. O termo também foi alterado no console e na API do Detective.	25 de fevereiro de 2021
“Conta principal” é alterado para “conta de administrador”	O termo “conta principal” é alterado para “conta de administrador”. O termo também foi alterado no console e na API do Detective.	25 de fevereiro de 2021
Adicionados detalhes da atividade para o volume de fluxo do VPC do painel de perfil do e para o endereço IP da descoberta	Agora o painel de perfil Volume de fluxo do VPC do e para o endereço IP da descoberta permite a exibição de detalhes da atividade. Os detalhes da atividade estão disponíveis somente se a descoberta estiver associada a um único endereço IP. Os detalhes da atividade mostram o volume de cada combinação de portas, protocolo e direção.	25 de fevereiro de 2021

[A opção da API de não enviar e-mails de convite para contas-membro foi adicionada](#)

Ao usar a API do Detective para adicionar contas-membro, as contas de administrador podem optar por não enviar e-mails de convite para contas-membro.

25 de fevereiro de 2021

[Novos detalhes da atividade no painel de perfil do volume geral de chamadas de API em perfis de endereço IP](#)

Agora você pode exibir detalhes da atividade dos endereços IP no painel de perfil Volume geral de chamadas de API. Os detalhes da atividade mostram o número de chamadas bem-sucedidas e malsucedidas para cada recurso que emitiu a chamada a partir do endereço IP.

23 de fevereiro de 2021

[Novo painel de perfil do volume geral de fluxo do VPC em perfis de endereço IP](#)

Agora o perfil de endereço IP contém o painel de perfil Volume geral de fluxo do VPC. O painel de perfil mostra o volume do tráfego de fluxo do VPC de e para o endereço IP. Você pode exibir detalhes da atividade para mostrar o volume de cada instância do EC2 com a qual o endereço IP se comunicou.

21 de janeiro de 2021

[Adicionada a página de
Resumo do Detective](#)

A página Resumo do Detective contém visualizações para orientar os analistas até as entidades de interesse com base na geolocalização, no número de chamadas de API e no volume de tráfego do Amazon EC2.

21 de janeiro de 2021

[Atualizou a opção de passar
da Amazon para Detective
GuardDuty](#)

Em GuardDuty, a opção Investigar em Detective é movida do menu Ações para o painel de detalhes da descoberta. Ele exibe uma lista de entidades relacionadas. Se o tipo de descoberta for compatível, a lista também incluirá a descoberta. Você poderá optar por navegar até o perfil de uma entidade ou o perfil de uma descoberta.

15 de janeiro de 2021

[Adicionada a opção para
definir a janela de detalhes da
atividade para o escopo de
tempo padrão](#)

Nos detalhes da atividade de Volume geral de chamadas de API e Volume geral de fluxo do VPC, você pode definir a janela de tempo dos detalhes da atividade como o escopo de tempo padrão do perfil.

15 de janeiro de 2021

[Adicionado o tratamento de intervalos de tempo de alto volume para entidades](#)

Foi adicionado um novo aviso para indicar quando uma entidade tem um ou mais intervalos de tempo de alto volume. Uma nova página de Entidades de alto volume exibe todos os intervalos de alto volume do escopo de tempo atual.

18 de dezembro de 2020

[A cota da conta-membro aumentou para 1.200](#)

Agora as contas principais podem convidar até 1.200 contas-membro para seu gráfico de comportamento. Anteriormente, a cota era de 1 mil.

11 de dezembro de 2020

[Valores para cotas de volume de dados do gráfico de comportamento foram adicionados](#)

Atualizamos as informações sobre as cotas de volume de dados do gráfico de comportamento para adicionar os valores específicos da cota.

11 de dezembro de 2020

[Adicionada a seleção de intervalo de tempo para detalhes da atividade no painel de perfil do volume geral de chamadas de API](#)

No painel Volume geral de fluxo da API, agora você pode exibir detalhes da atividade para qualquer intervalo de tempo selecionado. O painel exibe inicialmente uma opção para mostrar os detalhes da atividade no escopo de tempo.

29 de setembro de 2020

Adicionada a seleção de intervalo de tempo para detalhes da atividade no painel de perfil do volume geral de fluxos do VPC	No painel Volume geral de fluxo do VPC, você pode exibir detalhes da atividade de um único intervalo de tempo a partir do gráfico. Para exibir os detalhes do intervalo de tempo, escolha o intervalo de tempo.	25 de setembro de 2020
Nova sessão de função e entidades de usuário federado	Agora o Detective permite que você explore e investigue e a autenticação federada. Você pode ver quais recursos assumiram cada função e quando essas autenticações ocorreram.	17 de setembro de 2020
Atualizações no gerenciamento do escopo de tempo	Removida a opção de bloquear ou desbloquear o escopo de tempo. Fica sempre bloqueado. No perfil de uma descoberta, um aviso é exibido se o escopo de tempo for diferente da janela de tempo da descoberta.	4 de setembro de 2020
O cabeçalho do perfil permanece visível enquanto você percorre um perfil	Nos perfis, o tipo, o identificador e o escopo de tempo permanecem visíveis à medida que você percorre os painéis de perfil em uma guia. Quando as guias não estão visíveis, você pode usar a lista suspensa de guias na trilha de navegação para navegar até uma guia diferente.	4 de setembro de 2020

[Pesquisar sempre exibe os resultados da pesquisa](#)

Quando você realiza uma pesquisa, ela agora exibe os resultados na página Pesquisar. A partir dos resultados, você pode migrar para o perfil de uma descoberta ou de uma entidade.

27 de agosto de 2020

[Adições aos critérios permitidos para pesquisas](#)

Os critérios permitidos para pesquisas foram expandidos. Você pode pesquisar AWS usuários e AWS funções por nome. Você pode usar o ARN para pesquisar descobertas, AWS funções, AWS usuários e instâncias do EC2.

27 de agosto de 2020

[Links para outros consoles a partir dos painéis de perfil](#)

No painel de perfil Detalhes da instância do EC2, o identificador da instância do EC2 está vinculado ao console do Amazon EC2. Nos painéis de perfil Detalhes do usuário e Detalhes da função, o nome do usuário e o nome da função estão vinculados ao console do IAM.

14 de agosto de 2020

[Detalhes da atividade dos dados de fluxo do VPC](#)

Agora o painel de perfil Volume geral de fluxo do VPC fornece acesso aos detalhes da atividade. Os detalhes da atividade mostram o fluxo de tráfego entre endereços IP e uma instância do EC2 durante um período selecionado.

23 de julho de 2020

[Agora as contas-membro podem ver seu uso e custo projetado](#)

Agora as contas-membro podem visualizar suas próprias informações de uso. Para contas-membro, a página Uso mostra a quantidade da ingestão de dados em cada gráfico de comportamento para o qual elas contribuem. As contas-membro também podem ver o custo projetado para 30 dias.

26 de maio de 2020

[Agora a avaliação gratuita é por conta em vez de por gráfico de comportamento](#)

Agora cada conta do Amazon Detective recebe uma avaliação gratuita separada em cada região. A avaliação gratuita começa quando a conta habilita o Detective ou na primeira vez em que a conta é habilitada como conta-membro.

26 de maio de 2020

[Novos scripts Python de código aberto em GitHub](#)

O novo [amazon-detective-multiaccount-scripts](#) repositório GitHub fornece scripts Python de código aberto que você pode usar para gerenciar gráficos de comportamento em todas as regiões. Você pode habilitar o Detective, adicionar e remover contas-membro e desabilitar o Detective.

21 de janeiro de 2020

[Introdução ao Amazon Detective](#)

O Detective usa machine learning e visualizações específicas para ajudar você a analisar e investigar problemas de segurança em seus workloads da Amazon Web Services (AWS).

2 de dezembro de 2019

O conteúdo do Guia de Administração de Detectives agora está consolidado no Guia do Usuário de Detectives.

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.