aws

Guia GuardDuty do usuário da Amazon

Amazon GuardDuty

Amazon GuardDuty: Guia GuardDuty do usuário da Amazon

Table of Contents

O que é a Amazon GuardDuty?

GuardDuty A Amazon é um serviço de monitoramento de segurança que analisa e processaFontes de dados fundamentais, como eventos de AWS CloudTrail gerenciamento, registros de AWS CloudTrail eventos, registros de fluxo de VPC (de instâncias do Amazon EC2) e registros de DNS. Ele também processa recursos como registros de auditoria do Kubernetes, atividade de login do RDS, registros do S3, volumes do EBS, monitoramento de runtime e registros de atividades da rede Lambda. Ele usa feeds de inteligência contra ameaças, como listas de endereços IP e domínios mal-intencionados, e machine learning para identificar atividades inesperadas, mal-intencionadas e possivelmente não autorizadas no seu ambiente da AWS. Isso pode incluir problemas como escalonamentos de privilégios, uso de credenciais expostas, comunicação com endereços IP, URLs ou domínios mal-intencionados, presença de malware nas instâncias e workloads de contêiner do Amazon EC2 ou descoberta de padrões incomuns de eventos de login em seu banco de dados. Por exemplo, GuardDuty pode detectar instâncias EC2 comprometidas e cargas de trabalho de contêineres servindo malware ou minerando bitcoins. Ele também monitora o comportamento de acesso à conta da AWS em busca de sinais de comprometimento, como implantações de infraestrutura não autorizadas, instâncias implantadas em uma região nunca usada antes, ou chamadas de API incomuns, como uma alteração na política de senhas para reduzir a força da senha.

GuardDuty informa você sobre o status do seu AWS ambiente produzindo descobertas de segurança que você pode visualizar no GuardDuty console ou por meio da Amazon EventBridge. GuardDuty também fornece suporte para você exportar suas descobertas para um bucket do Amazon Simple Storage Service (S3) e integrá-las a outros serviços, como Detective. AWS Security Hub

Preços para GuardDuty

Para obter informações sobre GuardDuty preços, consulte Amazon GuardDuty Pricing.

Acessando GuardDuty

Você pode trabalhar com GuardDuty qualquer uma das seguintes formas:

GuardDuty console

- https://console.aws.amazon.com/guardduty

O console é uma interface baseada em navegador para acesso e uso do GuardDuty. O GuardDuty console fornece acesso à sua GuardDuty conta, dados e recursos.

Ferramentas da linha de comando da AWS

Com as ferramentas de linha de AWS comando, você pode emitir comandos na linha de comando do seu sistema para realizar GuardDuty tarefas e AWS tarefas. As ferramentas da linha de comando são úteis se você quiser criar scripts que realizem tarefas.

Para obter informações sobre a instalação e o uso da AWS CLI, consulte o Guia do usuário da AWS Command Line Interface. Para ver os AWS CLI comandos disponíveis para GuardDuty, consulte a referência de comandos da CLI.

GuardDuty API HTTPS

Você pode acessar GuardDuty e AWS programaticamente usando a API GuardDuty HTTPS, que permite emitir solicitações HTTPS diretamente para o serviço. Para obter mais informações, consulte a GuardDuty Referência da API.

SDKs da AWS

A AWS fornece SDKs (kits de desenvolvimento de software) que consistem em bibliotecas e códigos de exemplo para várias linguagens de programação e plataformas (Java, Python, Ruby, .NET, iOS e Android, entre outras). Os SDKs são uma forma conveniente de criar acesso programático ao GuardDuty. Para obter informações sobre os SDKs AWS, incluindo como fazer download e instalá-los, consulte Ferramentas da Amazon Web Services.

Começando com GuardDuty

Este tutorial fornece uma introdução prática ao. GuardDuty Os requisitos mínimos para habilitação GuardDuty como conta independente ou como GuardDuty administrador AWS Organizations são abordados na Etapa 1. As etapas 2 a 5 abrangem o uso de recursos adicionais recomendados por GuardDuty para aproveitar ao máximo suas descobertas.

Tópicos

Antes de começar

GuardDuty é um serviço de detecção de ameaças que monitora Fontes de dados fundamentais registros de AWS CloudTrail eventos, eventos AWS CloudTrail de gerenciamento, registros de fluxo da Amazon VPC e registros de DNS. GuardDuty também analisa os recursos associados a seus tipos de proteção somente se você os ativar separadamente. Os atributos incluem logs de auditoria do Kubernetes, atividade de login do RDS, logs do S3, volumes do EBS, monitoramento de runtime e registros de atividades de rede do Lambda. O uso dessas fontes de dados e recursos (se ativado) GuardDuty gera descobertas de segurança para sua conta.

Depois de habilitar GuardDuty, ele começa a monitorar seu ambiente. Você pode desativar GuardDuty qualquer conta em qualquer região, a qualquer momento. Isso interromperá o processamento das fontes GuardDuty de dados fundamentais e de quaisquer recursos que tenham sido ativados separadamente.

Não é necessário habilitar explicitamente nenhuma das opções de Fontes de dados fundamentais. A Amazon GuardDuty extrai fluxos independentes de dados diretamente desses serviços. Para uma nova GuardDuty conta, todos os tipos de proteção disponíveis que são suportados em um Região da AWS são ativados e incluídos no período de teste gratuito de 30 dias por padrão. Você pode desabilitar um ou todos eles. Se você já é um GuardDuty cliente, pode optar por ativar qualquer um

ou todos os planos de proteção disponíveis no seu Região da AWS. Para obter mais informações, consulte Recursos associados a cada tipo de proteção em GuardDuty.

Ao ativar GuardDuty, considere os seguintes itens:

- GuardDuty é um serviço regional, o que significa que qualquer um dos procedimentos de configuração que você segue nesta página deve ser repetido em cada região com a qual você deseja monitorar GuardDuty.

  É altamente recomendável que você habilite GuardDuty em todas as AWS regiões suportadas. Isso permite GuardDuty gerar descobertas sobre atividades não autorizadas ou incomuns, mesmo em regiões que você não está usando ativamente. Isso também permite GuardDuty monitorar AWS CloudTrail eventos para AWS serviços globais, como o IAM. Se não GuardDuty estiver habilitado em todas as regiões suportadas, sua capacidade de detectar atividades que envolvam serviços globais será reduzida. Para obter uma lista completa das regiões onde GuardDuty está disponível, consulteRegiões e endpoints.
- Qualquer usuário com privilégios de administrador em uma AWS conta pode habilitar GuardDuty, no entanto, seguindo a melhor prática de segurança do menor privilégio, é recomendável criar uma função, usuário ou grupo do IAM para gerenciar GuardDuty especificamente. Para obter informações sobre as permissões necessárias para habilitar, GuardDuty consultePermissões necessárias para habilitar o GuardDuty.
- Quando você ativa GuardDuty pela primeira vez em qualquer um Região da AWS, por padrão, ele também ativa todos os tipos de proteção disponíveis que são suportados nessa região, incluindo a Proteção contra Malware. GuardDuty cria uma função vinculada ao serviço para sua conta chamada. `AWSServiceRoleForAmazonGuardDuty` Essa função inclui as permissões e as políticas de confiança que GuardDuty permitem consumir e analisar eventos diretamente do Fontes de dados fundamentais para gerar descobertas de segurança. A Proteção contra malware cria outra função vinculada ao serviço para sua conta, chamada `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Essa função inclui as permissões e as políticas de confiança que permitem que o Malware Protection realize verificações sem agentes para detectar malware em sua conta. GuardDuty Ele permite GuardDuty criar um instantâneo do volume do EBS em sua conta e compartilhar esse instantâneo com a GuardDuty conta de serviço. Para ter mais informações, consulte Permissões de função vinculadas ao serviço para GuardDuty. Para obter mais informações sobre as funções vinculadas a um serviço, consulte Como usar funções vinculadas a serviços.

- Quando você ativa GuardDuty pela primeira vez em qualquer região, sua AWS conta é automaticamente inscrita em um teste GuardDuty gratuito de 30 dias para essa região.

Etapa 1: habilitar a Amazon GuardDuty

O primeiro passo para usar GuardDuty é habilitá-lo em sua conta. Uma vez ativado, GuardDuty começará imediatamente a monitorar as ameaças à segurança na região atual.

Se você quiser gerenciar GuardDuty descobertas para outras contas em sua organização como GuardDuty administrador, você deve adicionar contas de membros e GuardDuty habilitá-las também. Escolha uma opção para saber como habilitar GuardDuty para seu ambiente.

Standalone account environment

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/
2. Escolha Começar.
3. Escolha Ativar GuardDuty.

Multi-account environment

> **Important**
>
> Como pré-requisitos para esse processo, você deve estar na mesma organização de todas as contas que deseja gerenciar e ter acesso à conta de AWS Organizations gerenciamento para delegar um administrador dentro da sua organização. GuardDuty Permissões adicionais podem ser necessárias para delegar um administrador. Para obter mais informações, consulte Permissões necessárias para designar uma conta de administrador delegado GuardDuty .

Para designar uma conta de administrador delegado GuardDuty

1. Abra o AWS Organizations console em https://console.aws.amazon.com/organizations/, usando a conta de gerenciamento.
2. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   GuardDuty Já está habilitado em sua conta?

- Se ainda não GuardDuty estiver habilitado, você pode selecionar Começar e designar um administrador GuardDuty delegado na página Bem-vindo ao GuardDuty.
- Se GuardDuty estiver ativado, você poderá designar um administrador GuardDuty delegado na página Configurações.

3. Insira o ID da AWS conta de doze dígitos da conta que você deseja designar como administrador GuardDuty delegado da organização e escolha Delegar.

> **Note**
>
> Se ainda não GuardDuty estiver habilitado, a designação de um administrador delegado GuardDuty habilitará essa conta na sua região atual.

Para adicionar contas-membro

Esse procedimento abrange a adição de contas de membros a uma conta de administrador GuardDuty delegado por meio AWS Organizations de. Também é possível adicionar membros por convite. Para saber mais sobre os dois métodos de associação de membros em GuardDuty, consulte[Gerenciando várias contas na Amazon GuardDuty](#).

1. Faça login na conta de administrador delegado
2. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
3. No painel de navegação, escolha Settings (Configurações) e selecione Accounts (Contas).

   A tabela de contas exibe todas as contas na organização.
4. Selecione as contas que deseja adicionar como membros marcando a caixa de seleção ao lado do ID da conta. Depois, no menu Ação, selecione Adicionar membro.

> **Tip**
>
> Você pode automatizar a inclusão de novas contas como membros habilitando o atributo de habilitação automática. No entanto, isso se aplica somente às contas que ingressam na sua organização após a habilitação do atributo.

Etapa 2: gerar descobertas de amostra e explorar as operações básicas

Quando GuardDuty descobre um problema de segurança, ele gera uma descoberta. Uma GuardDuty descoberta é um conjunto de dados contendo detalhes relacionados a esse problema de segurança exclusivo. Os detalhes da descoberta podem ser usados para ajudar a investigar o problema.

GuardDuty suporta a geração de amostras de descobertas com valores de espaço reservado, que podem ser usados para testar a GuardDuty funcionalidade e se familiarizar com as descobertas antes de precisar responder a um problema de segurança real descoberto por. GuardDuty Siga o guia abaixo para gerar exemplos de descobertas para cada tipo de descoberta disponível em GuardDuty. Para obter outras formas de gerar exemplos de descobertas, incluindo a geração de um evento de segurança simulado em sua conta, consulteDescobertas de exemplo.

Para criar e explorar descobertas de amostra

1. No painel de navegação, selecione Configurações.
2. Na página Settings, em Sample findings, escolha Generate sample findings.
3. No painel de navegação, escolha Resumo para visualizar os insights sobre as descobertas geradas em seu AWS ambiente. Para obter mais informações sobre os componentes do painel de resumo, consulte Painel de resumo.
4. No painel de navegação, selecione Descobertas. As descoberta de amostra são exibidas na página Descobertas atuais com o prefixo [SAMPLE].
5. Selecione uma descoberta na lista para exibir os detalhes dela.

    - Os diversos campos de informações disponíveis podem ser revisados no painel de detalhes da descoberta. Tipos diferentes de descobertas podem ter campos diferentes. Para obter mais informações sobre os campos disponíveis em todos os tipos de descoberta, consulte Detalhes da descoberta. No painel de detalhes, você pode utilizar as seguintes ações:

        - Na parte superior do painel, selecione o ID da descoberta para abrir os detalhes completos do JSON da descoberta. Nesse painel também é possível baixar o arquivo JSON completo. O JSON contém algumas informações adicionais não incluídas na visualização do console e é o formato que outras ferramentas e serviços podem ingerir.
        - Veja a seção Recurso afetado. Em uma descoberta real, as informações aqui ajudarão você a identificar um recurso em sua conta que deve ser investigado e incluirão links para os recursos apropriados AWS Management Console para uso.

- Selecione os ícones de lupa + ou - para criar um filtro inclusivo ou exclusivo para esse detalhe. Para obter mais informações sobre os filtros de descobertas, consulte Filtrar descobertas.

6. Arquive todas as suas descobertas de amostra

   a. Selecione todas as descobertas marcando a caixa de seleção na parte superior da lista.

   b. Desmarque todas as descobertas que você deseja manter.

   c. Selecione o menu Ações e, em seguida, selecione Arquivar para ocultar as descobertas de amostra.

> **Note**
>
> Selecione Atual para visualizar as descobertas arquivadas e, em seguida, Arquivado para alternar a visualização das descobertas.

Etapa 3: Configurar a exportação de GuardDuty descobertas para um bucket do Amazon S3

GuardDuty recomenda definir configurações para exportar descobertas porque permite exportar suas descobertas para um bucket do S3 para armazenamento indefinido além do período de retenção de 90 dias. GuardDuty Isso permite que você mantenha registros das descobertas ou acompanhe problemas em seu AWS ambiente ao longo do tempo. O processo descrito aqui orienta a configuração de um novo bucket do S3 e a criação de uma nova chave do KMS para criptografar as descobertas de dentro do console. Para obter mais informações sobre isso, incluindo como usar seu próprio bucket existente ou um bucket em outra conta, consulte Exportar descobertas.

Para configurar a opção exportar descobertas do S3

1. Para criptografar as descobertas, você precisará de uma chave KMS com uma política que permita GuardDuty usar essa chave para criptografia. As etapas a seguir ajudarão a criar uma nova chave do KMS. Se você estiver usando uma chave KMS de outra conta, precisará aplicar a política de chaves fazendo login no Conta da AWS proprietário da chave. A região de sua chave do KMS e do bucket do S3 deve ser a mesma. No entanto, é possível usar esse mesmo bucket e o mesmo par de chaves para cada região de onde as descobertas serão exportadas.

   a. Abra o AWS KMS console em https://console.aws.amazon.com/kms.

b. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.

c. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas de cliente).

d. Escolha Create key (Criar chave).

e. Escolha Simétrico em Tipo de chave e, em seguida, escolha Próximo.

> **Note**
>
> As etapas detalhadas da criação de sua chave do KMS podem ser consultadas em Criar chaves no Guia do Desenvolvedor do AWS Key Management Service .

f. Forneça um Alias para sua chave e escolha Próximo.

g. Escolha Próximo e, novamente, escolha Próximo para aceitar as permissões padrão de administração e uso.

h. Depois de Revisar a configuração, escolha Concluir para criar a chave.

i. Na página Chaves gerenciadas pelo cliente, escolha o alias de sua chave.

j. Na seção Política de chaves, selecione Mudar para visualização da política.

k. Escolha Editar e adicione a seguinte política de chaves à sua chave KMS, concedendo GuardDuty acesso à sua chave. Essa declaração permite GuardDuty usar somente a chave à qual você adiciona essa política. Durante a edição da política de chaves, verifique se a sintaxe JSON é válida. Se você adicionar a declaração antes da declaração final, adicione uma vírgula após o colchete de fechamento.

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "arn:aws:kms:Region1:444455556666:key/KMSKeyId",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333",
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:111122223333:detector/SourceDetectorID"
        }
    }
```

```
}
```

Substitua *Region1* pela região da sua chave do KMS. Substitua *444455556666* pelo proprietário da Conta da AWS chave KMS. KeyIdSubstitua o *KMS* pelo ID da chave KMS que você escolheu para criptografia. Para identificar todos esses valores — região e ID da chave Conta da AWS, visualize o ARN da sua chave KMS. Para localizar o ARN da chave, consulte Como localizar o ID e o ARN da chave.

Da mesma forma, substitua *111122223333* pelo da conta. Conta da AWS GuardDuty Substitua *Região2* pela Região da GuardDuty conta. Substitua o *SourceDetectorID* pelo ID do detector da GuardDuty conta da *Região 2*.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

l. Selecione Salvar.

2. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
3. No painel de navegação, selecione Configurações.
4. Em Opções de exportação de descobertas, escolha Configure agora.
5. Selecione Novo bucket. Forneça um nome exclusivo para o seu bucket do S3.
6. (Opcional) Você pode testar suas novas configurações de exportação gerando descobertas de amostra. No painel de navegação, selecione Configurações.
7. Em Descobertas de amostra, escolha Gerar descobertas de amostra. As novas descobertas de amostra aparecerão como entradas no bucket do S3 criado por GuardDuty em até cinco minutos.

Etapa 4: configurar alertas de GuardDuty busca por meio do SNS

GuardDuty se integra à Amazon EventBridge, que pode ser usada para enviar dados de descobertas para outros aplicativos e serviços para processamento. Com EventBridge você pode usar GuardDuty as descobertas para iniciar respostas automáticas às suas descobertas conectando eventos de busca a destinos como AWS Lambda funções, automação do Amazon EC2 Systems Manager, Amazon Simple Notification Service (SNS) e muito mais.

Neste exemplo, você criará um tópico do SNS para ser o alvo de uma EventBridge regra e, em seguida, usará EventBridge para criar uma regra que capture dados de descobertas. GuardDuty A regra resultante encaminha os detalhes da descoberta para um endereço de e-mail. Para saber

como você pode enviar descobertas para o Slack ou o Amazon Chime e também modificar os tipos de descobertas para os quais os alertas são enviados, consulte Configurar um tópico e um endpoint do Amazon SNS.

Para criar um tópico do SNS para seus alertas de descobertas

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. No painel de navegação, escolha Tópicos.
3. Selecione Criar tópico.
4. Em Tipo, selecione Padrão.
5. Em Nome, digite **`GuardDuty`**.
6. Selecione Criar tópico. A seção Detalhes do novo tópico será aberta.
7. Na seção Subscriptions (Inscrições), escolha Create subscription (Criar inscrição).
8. Em Protocolo, escolha Email.
9. Para Endpoint, insira o endereço de e-mail que deve receber as notificações.
10. Selecione Criar assinatura.

    É necessário confirmar a assinatura por e-mail após a criação da assinatura.
11. Para conferir se há uma mensagem de assinatura, acesse sua caixa de entrada de e-mail e, na mensagem de assinatura, escolha Confirmar assinatura.

> **Note**
>
> Para conferir o status do e-mail de confirmação, acesse o console do SNS e escolha Assinaturas.

Para criar uma EventBridge regra para capturar GuardDuty descobertas e formatá-las

1. Abra o EventBridge console em https://console.aws.amazon.com/events/.
2. No painel de navegação, escolha Regras.
3. Selecione Criar regra.
4. Insira um nome e uma descrição para a regra.

   Uma regra não pode ter o mesmo nome que outra na mesma Região e barramento de eventos.
5. Em Event Bus (Barramento de eventos), escolha default (padrão).

6. Em Rule type (Tipo de regra), selecione Rule with an event pattern (Regra com um padrão de evento).
7. Selecione Next (Próximo).
8. Em Origem de eventos, escolha Eventos da AWS .
9. Na seção Padrão de eventos, selecione Formulário de padrão de eventos.
10. Em Fonte do evento, selecione Serviços da AWS .
11. Em Serviço da AWS , escolha GuardDuty.
12. Em Tipo de evento, escolha GuardDutyLocalizar.
13. Selecione Next (Próximo).
14. Em Tipos de destino, escolha Serviço da AWS .
15. Em Selecionar um destino, escolha Tópico do SNS e, em Tópico, escolha o nome do tópico do SNS que você criou anteriormente.
16. Na seção Configurações adicionais, para Configurar entrada de destino, escolha Transformador de entrada.

    Adicionar um transformador de entrada formata os dados de localização JSON enviados GuardDuty em uma mensagem legível por humanos.
17. Escolha Configure input transformer.
18. Na seção Transformador de entrada de destino, em Caminho de entrada, cole este código:

```
{
  "severity": "$.detail.severity",
  "Finding_ID": "$.detail.id",
  "Finding_Type": "$.detail.type",
  "region": "$.region",
  "Finding_description": "$.detail.description"
}
```

19. Para formatar o e-mail, em Modelo, cole o código a seguir e certifique-se de substituir o texto em vermelho pelos valores apropriados à sua região:

```
"You have a severity severity GuardDuty finding type Finding_Type in
 the Region_Name Region."
"Finding Description:"
```

```
"Finding_Description."
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=region#/findings?search=id%3DFinding_ID"
```

20. Selecione a opção Confirmar.
21. Escolha Próximo.
22. (Opcional) Insira uma ou mais tags para a regra. Para obter mais informações, consulte as EventBridge tags da Amazon no Guia EventBridge do usuário da Amazon.
23. Selecione Next (Próximo).
24. Analise os detalhes da regra e selecione Criar regra.
25. (Opcional) Teste sua nova regra gerando descobertas de exemplo com o processo na Etapa 2. Você receberá um e-mail para cada descoberta de amostra gerada.

Próximas etapas

Ao continuar usando GuardDuty, você entenderá os tipos de descobertas que são relevantes para seu ambiente. Sempre que receber uma nova descoberta, você pode encontrar informações, incluindo recomendações de remediação sobre essa descoberta, selecionando Saiba mais na descrição da descoberta no painel de detalhes da descoberta ou pesquisando o nome da descoberta em Tipos de descoberta.

Os recursos a seguir ajudarão você a se ajustar GuardDuty para que possam fornecer as descobertas mais relevantes para seu AWS ambiente:

- Para classificar facilmente as descobertas com base em critérios específicos, como ID da instância, ID da conta, nome do bucket do S3 e muito mais, você pode criar e salvar filtros nele GuardDuty. Para ter mais informações, consulte Filtrar descobertas.
- Se você estiver recebendo descobertas sobre o comportamento esperado em seu ambiente, poderá arquivar automaticamente as descobertas com base nos critérios definidos com as regras de supressão.
- Para evitar que descobertas sejam geradas a partir de um subconjunto de IPs confiáveis ou para que os IPs de GuardDuty monitoramento estejam fora do escopo normal de monitoramento, você pode configurar listas de IPs confiáveis e de ameaças.

Conceitos e terminologia

Ao começar a usar a Amazon GuardDuty, você pode se beneficiar ao aprender sobre seus principais conceitos.

Conta

Uma conta padrão da Amazon Web Services (AWS) que contém seus AWS recursos. Você pode entrar AWS com sua conta e ativar GuardDuty.

Você também pode convidar outras contas para ativar GuardDuty e se associar à sua AWS conta em GuardDuty. Se seus convites forem aceitos, sua conta será designada como conta GuardDuty de administrador e as contas adicionadas se tornarão suas contas de membros. Em seguida, você pode visualizar e gerenciar as GuardDuty descobertas dessas contas em nome delas.

Os usuários da conta de administrador podem configurar GuardDuty , visualizar e gerenciar GuardDuty as descobertas de sua própria conta e de todas as contas de membros. Você pode ter até 10.000 contas de membros em GuardDuty.

Os usuários das contas dos membros podem configurar GuardDuty , visualizar e gerenciar GuardDuty descobertas em suas contas (por meio do console GuardDuty de gerenciamento ou GuardDuty da API). Os usuários de contas de membro não podem visualizar ou gerenciar descobertas nas contas de outros membros.

Uma AWS conta não pode ser uma conta de GuardDuty administrador e uma conta de membro ao mesmo tempo. Uma conta da AWS pode aceitar apenas um convite de associação. Aceitar um convite de associação é opcional.

Para ter mais informações, consulte Gerenciando várias contas na Amazon GuardDuty.

Detector

Todas as GuardDuty descobertas estão associadas a um detector, que é um objeto que representa o GuardDuty serviço. O detector é uma entidade regional e é necessário um detector exclusivo em cada um Região da AWS em que GuardDuty opera. Quando você ativa GuardDuty em uma região, um novo detector com um DetectorID alfanumérico exclusivo de 32 é gerado nessa região. O formato de um detectorId é `12abc34d567e8fa901bc2d34e56789f0`.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

> **Note**
>
> Em ambientes de várias contas, todas as descobertas de contas-membro são acumuladas no detector da conta de administrador.

Algumas GuardDuty funcionalidades são configuradas por meio do detector, como a configuração da frequência de notificação de CloudWatch eventos e a ativação ou desativação de fontes de dados opcionais GuardDuty para processamento.

Fonte de dados

A origem ou a localização de um conjunto de dados. Para detectar uma atividade não autorizada ou inesperada em seu AWS ambiente. GuardDuty analisa e processa dados de registros de eventos, AWS CloudTrail eventos de AWS CloudTrail gerenciamento, eventos de AWS CloudTrail dados para S3, registros de fluxo de VPC, registros de DNS, registros de auditoria do EKS, monitoramento de atividades de login do RDS e volumes do EBS. Para ter mais informações, consulte Fontes de dados fundamentais.

Atributo

Um objeto de recurso configurado para seu plano de GuardDuty proteção ajuda a detectar uma atividade não autorizada ou inesperada em seu AWS ambiente. Cada plano GuardDuty de proteção configura o objeto de recurso correspondente para analisar e processar dados. Alguns dos objetos de atributo incluem logs de auditoria do EKS, monitoramento de atividades de login do RDS e volumes do EBS. Para ter mais informações, consulte Ativação de recursos em GuardDuty.

Descoberta

Um possível problema de segurança descoberto pelo GuardDuty. Para ter mais informações, consulte Entendendo as GuardDuty descobertas da Amazon.

As descobertas são exibidas no GuardDuty console e contêm uma descrição detalhada do problema de segurança. Você também pode recuperar suas descobertas geradas chamando as operações GetFindingse da ListFindingsAPI.

Você também pode ver suas GuardDuty descobertas por meio de CloudWatch eventos da Amazon. GuardDuty envia descobertas para a Amazon CloudWatch por meio do protocolo HTTPS. Para ter mais informações, consulte Criação de respostas personalizadas às GuardDuty descobertas com a Amazon CloudWatch Events.

Opções de verificação

Quando a Proteção contra GuardDuty Malware está ativada, ela permite que você especifique quais instâncias do Amazon EC2 e volumes do Amazon Elastic Block Store (EBS) devem ser verificados ou ignorados. Esse atributo permite que você adicione as tags existentes associadas às suas instâncias do EC2 e ao volume do EBS a uma lista de tags de inclusão ou de exclusão. Os recursos associados às tags que você adiciona a uma lista de tags de inclusão são verificados em busca de malware, e aqueles adicionados a uma lista de tags de exclusão não são examinados. Para ter mais informações, consulte Opções de verificação com tags definidas pelo usuário.

Retenção de snapshots

Quando a Proteção contra GuardDuty Malware está ativada, ela oferece a opção de reter os instantâneos dos volumes do EBS em sua AWS conta. GuardDuty gera os volumes de réplica do EBS com base nos instantâneos dos seus volumes do EBS. Você pode reter os snapshots dos seus volumes do EBS somente se a verificação da Proteção contra malware detectar malware nos volumes de réplica do EBS. Se nenhum malware for detectado nos volumes de réplica do EBS, GuardDuty excluirá automaticamente os instantâneos dos seus volumes do EBS, independentemente da configuração de retenção de instantâneos. Para ter mais informações, consulte Retenção de snapshots.

Regra de supressão

As regras de supressão permitem criar combinações muito específicas de atributos para suprimir descobertas. Por exemplo, você pode definir uma regra por meio do GuardDuty filtro para arquivar automaticamente `Recon:EC2/Portscan` somente dessas instâncias em uma VPC específica, executando uma AMI específica ou com uma tag EC2 específica. Essa regra resultaria em descobertas de varredura de portas sendo arquivadas automaticamente a partir das instâncias que atendem aos critérios. No entanto, ele ainda permite alertar se GuardDuty detectar essas instâncias conduzindo outras atividades maliciosas, como mineração de criptomoedas.

As regras de supressão definidas na conta do GuardDuty administrador se aplicam às contas dos GuardDuty membros. GuardDuty as contas dos membros não podem modificar as regras de supressão.

Com as regras de supressão, GuardDuty ainda gera todas as descobertas. As regras de supressão fornecem supressão de descobertas e mantêm um histórico completo e imutável de toda a atividade.

Normalmente, as regras de supressão são usadas para ocultar descobertas determinadas como falsos positivos para o ambiente e reduzir o ruído de descobertas de baixo valor para que você possa se concentrar em ameaças maiores. Para ter mais informações, consulte Regras de supressão.

Lista de IPs confiáveis

Uma lista de endereços IP confiáveis para comunicação altamente segura com seu AWS ambiente. GuardDuty não gera descobertas com base em listas de IP confiáveis. Para ter mais informações, consulte Como trabalhar com listas de IPs confiáveis e listas de ameaças.

Lista de IPs de ameaças

Uma lista de endereços IP mal-intencionados conhecidos. Além de gerar descobertas devido a uma atividade potencialmente suspeita, GuardDuty também gera descobertas com base nessas listas de ameaças. Para ter mais informações, consulte Como trabalhar com listas de IPs confiáveis e listas de ameaças.

Ativação de recursos em GuardDuty

Quando você ativa a Amazon GuardDuty pela primeira vez ou ativa um tipo de proteção dentro dela GuardDuty, GuardDuty começa a processar o correspondente Fontes de dados fundamentais em seu AWS ambiente. GuardDuty usa essas fontes de dados para processar um fluxo de eventos, como registros de fluxo de VPC, registros de DNS e registros de AWS CloudTrail eventos e gerenciamento. Em seguida, ele analisa esses eventos para identificar possíveis ameaças à segurança e gera descobertas em sua conta.

Além das fontes de dados de log, GuardDuty você pode usar dados adicionais de outros AWS serviços em seu AWS ambiente para monitorar e analisar possíveis ameaças à segurança.

Habilitações de recursos

Ao adicionar GuardDuty proteções adicionais, por exemplo, Proteção S3, Monitoramento de Tempo de Execução ou Proteção EKS, você pode configurar o GuardDuty recurso correspondente ao tipo de proteção. Historicamente, GuardDuty as proteções eram chamadas `dataSources` nas APIs. No entanto, após março de 2023, os novos tipos de GuardDuty proteção agora estão configurados como `features` e não`dataSources`. GuardDuty ainda oferece suporte à configuração de tipos de proteção lançados antes de março de 2023, como `dataSources` por meio da API, mas novos tipos de proteção só estão disponíveis como`features`.

Se você gerencia os tipos de GuardDuty configuração e proteção por meio do console, não será diretamente afetado por essa alteração e não precisará realizar nenhuma ação. A ativação do recurso afeta o comportamento das APIs que são invocadas para ativar GuardDuty ou proteger os tipos internos. GuardDuty Para obter mais informações, consulte GuardDuty Mudanças na API.

GuardDuty Mudanças na API em março de 2023

As GuardDuty APIs configuram recursos de proteção que não pertencem à lista deFontes de dados fundamentais. Um objeto de recurso contém detalhes do recurso, como nome e status do recurso, e pode conter configurações adicionais para alguns dos recursos. Essa migração afeta as seguintes APIs na Amazon GuardDuty API Reference:

- CreateDetector
- GetDetector

- UpdateDetector
- GetMemberDetectors
- UpdateMemberDetectors
- DescribeOrganizationConfiguration
- UpdateOrganizationConfiguration
- GetRemainingFreeTrialDays
- GetUsageStatistics

Habilitação de recursos em comparação com fontes de dados

Historicamente, todos os GuardDuty recursos eram passados por um `dataSources` objeto na API. A partir de março de 2023, GuardDuty prefere o `features` objeto em vez do `dataSources` objeto na API. Todas as fontes de dados anteriores têm recursos correspondentes, mas os recursos mais novos podem não ter fontes de dados correspondentes.

A lista a seguir mostra a comparação `dataSources` entre um `features` objeto quando passado por uma API:

- O `dataSources` objeto contém objetos para cada tipo de proteção e seu status. O `features` objeto é uma lista de recursos disponíveis que correspondem a cada tipo de proteção contido nele GuardDuty.

  A partir de março de 2023, a ativação de recursos será a única forma de configurar novos GuardDuty recursos em seu AWS ambiente.
- O `dataSources` esquema na solicitação ou resposta da API é o mesmo em todos os Região da AWS lugares GuardDuty disponíveis. No entanto, nem todos os atributos podem estar disponíveis em cada região. Portanto, os nomes dos recursos disponíveis podem diferir com base na região.

Entendendo como a habilitação de recursos funciona

As GuardDuty APIs continuarão retornando um `dataSources` objeto conforme aplicável e também retornarão um `features` objeto contendo as mesmas informações em um formato diferente. GuardDuty recursos lançados antes de março de 2023 estarão disponíveis por meio de `dataSources` objeto e `features` objeto. GuardDuty recursos lançados desde março de 2023 só estarão disponíveis por meio do `features` objeto. Você não pode criar ou atualizar um detector nem

descrever seu AWS Organizations uso `dataSources` e a notação de `features` objeto na mesma solicitação de API. Para ativar os tipos de GuardDuty proteção, você precisará migrar suas fontes de dados existentes para o `features` objeto usando as mesmas APIs que agora também incluem o `features` objeto.

> **Note**
>
> GuardDuty não adicionará uma nova fonte de dados após essa modificação.

GuardDuty descontinuou o uso de fontes de dados. No entanto, ele ainda suporta Fontes de dados fundamentais o. As GuardDuty melhores práticas recomendam usar a ativação de recursos para qualquer tipo de proteção que já esteja habilitado para sua conta. As melhores práticas também exigem o uso da habilitação de recursos ao habilitar um novo tipo de proteção para sua conta.

Incorporando alterações de habilitação de recursos

- Se você gerencia GuardDuty configurações por meio de APIs, SDKs ou AWS CloudFormation modelo e deseja habilitar possíveis novos GuardDuty recursos, precisará modificar seu código e modelo, respectivamente. Para obter mais informações, consulte as APIs atualizadas na Amazon GuardDuty API Reference.
- Para GuardDuty recursos configurados antes dessa atualização, você pode continuar usando as APIs, os SDKs ou AWS CloudFormation o modelo. No entanto, recomendamos que você mude para usar o `feature` objeto.

  Todas as fontes de dados têm um objeto de recurso equivalente. Para obter mais informações, consulte Mapeando `dataSources` para `features`.
- Atualmente, `additionalConfiguration` o `features` objeto está disponível apenas para determinados tipos de proteção.
  - Para esses tipos de proteção, se o seu recurso `AdditionalConfiguration` `status` estiver definido como`ENABLED`, mas a configuração do seu recurso não `status` estiver definida`ENABLED`, não GuardDuty tomará nenhuma ação nesse caso.
  - As seguintes APIs são afetadas por isso:
    - UpdateDetector
    - UpdateMemberDetectors
    - UpdateOrganizationConfiguration

Mapeando **`dataSources`** para **`features`**

A tabela a seguir mostra o mapeamento dos tipos de proteção`dataSources`, `features` e.

GuardDuty tipo de proteção	Nome da fonte de dados *	Nome do recurso
Logs de fluxo da VPC	`flowLogs` (somente leitura, não pode ser modificado)	`FLOW_LOGS` (somente leitura, não pode ser modificado)
Logs de DNS	`dnsLogs` (somente leitura, não pode ser modificado)	`DNS_LOGS` (somente leitura, não pode ser modificado)
CloudTrail eventos	`cloudLogs` (somente leitura, não pode ser modificado)	`CLOUD_LOGS` (somente leitura, não pode ser modificado)
S3	`s3Logs`	`S3_DATA_EVENTS`
Monitoramento do registro de auditoria EKS	`kubernetes.auditlogs`	`EKS_AUDIT_LOGS`
Proteção contra malware	`malwareProtection.scanEc2InstanceWithFindings.ebsVolumes`	`EBS_MALWARE_PROTECTION`
Eventos de login do RDS	GuardDuty fornece suporte somente à ativação de recursos para esses tipos de proteção.	`RDS_LOGIN_EVENTS`
EKS Runtime Monitoring		`EKS_RUNTIME_MONITORING`

GuardDuty tipo de proteção	Nome da fonte de dados *	Nome do recurso
Monitoramento de execução		`RUNTIME_MONITORING`

GuardDuty agente de segurança para clusters Amazon EKS		`EKS_RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT`
		
		`RUNTIME_MONITORING.additionalConfiguration.EKS_ADDON_MANAGEMENT`

GuardDuty agente de segurança para clusters Amazon ECS		`RUNTIME_MONITORING.additionalConfiguration.ECS_FARGATE_AGENT_MANAGEMENT`
Proteção do Lambda		`LAMBDA_NETWORK_LOGS`

*GetUsageStatistics usa seus próprios nomes de `dataSource`. Para ter mais informações, consulte Estimando GuardDuty o custo ou GetUsageStatistics.

Fontes de dados fundamentais

GuardDuty usa as fontes de dados básicas para detectar a comunicação com domínios e endereços IP maliciosos conhecidos e identificar comportamentos anômalos. Enquanto estão em trânsito dessas fontes para GuardDuty, todos os dados de registro são criptografados. GuardDutyextrai vários campos dessas fontes de registros para criação de perfil e detecção de anomalias e, em seguida, descarta esses registros.

As seções a seguir descrevem como GuardDuty usa cada fonte de dados compatível. Quando você ativa o GuardDuty seu Conta da AWS, GuardDuty automaticamente começa a monitorar essas fontes de registro.

Tópicos

AWS CloudTrail registros de eventos

AWS CloudTrail fornece um histórico de chamadas de AWS API para sua conta, incluindo chamadas de API feitas usando o AWS Management Console, os AWS SDKs, as ferramentas de linha de comando e determinados AWS serviços. CloudTrail também ajuda a identificar quais usuários e contas invocaram AWS APIs para serviços compatíveis CloudTrail, o endereço IP de origem de onde as chamadas foram invocadas e a hora em que as chamadas foram invocadas. Para obter mais informações, consulte O que é o AWS CloudTrail no Guia do usuário do AWS CloudTrail .

GuardDuty também monitora eventos CloudTrail de gerenciamento. Quando você ativa GuardDuty, ele começa a consumir eventos CloudTrail de gerenciamento diretamente CloudTrail por meio de um fluxo de eventos independente e duplicado e analisa seus CloudTrail registros de eventos. Não há cobrança adicional ao GuardDuty acessar os eventos registrados em CloudTrail.

GuardDuty não gerencia seus CloudTrail eventos nem afeta suas CloudTrail configurações existentes. Da mesma forma, suas CloudTrail configurações não afetam a forma como GuardDuty consome e processa os registros de eventos. Para gerenciar o acesso e a retenção de seus CloudTrail eventos, use o console CloudTrail de serviço ou a API. Para obter mais informações,

consulte Visualização de eventos com histórico de CloudTrail eventos no Guia AWS CloudTrail do usuário.

Como GuardDuty lida com eventos AWS CloudTrail globais

Para a maioria dos AWS serviços, os CloudTrail eventos são registrados no Região da AWS local em que são criados. Para serviços globais como AWS Identity and Access Management (IAM), AWS Security Token Service (AWS STS), Amazon Simple Storage Service (Amazon S3), Amazon e CloudFront Amazon Route 53 (Route 53), os eventos são gerados somente na região em que ocorrem, mas têm um significado global.

Quando GuardDuty consome eventos de serviço CloudTrail global com valor de segurança, como configurações de rede ou permissões de usuário, ele replica esses eventos e os processa em cada região em que você ativou. GuardDuty Esse comportamento ajuda a GuardDuty manter perfis de usuário e função em cada região, o que é vital para detectar eventos anômalos.

É altamente recomendável que você ative todos GuardDuty os Regiões da AWS que estão habilitados para o seu Conta da AWS. Isso ajuda a GuardDuty gerar descobertas sobre atividades não autorizadas ou incomuns, mesmo nas regiões que você pode não estar usando ativamente.

AWS CloudTrail eventos de gerenciamento

Os eventos de gerenciamento também são conhecidos como eventos do ambiente de gerenciamento. Esses eventos fornecem informações sobre as operações de gerenciamento que são realizadas nos recursos AWS da sua conta.

Veja a seguir exemplos de eventos de CloudTrail gerenciamento que GuardDuty monitoram:

- Configuração da segurança (operações da API `AttachRolePolicy` do IAM)
- Configuração de regras para roteamento de dados (por exemplo, operações de API `CreateSubnet` do Amazon EC2)
- Configurando o registro (operações de AWS CloudTrail `CreateTrail` API)

Logs de fluxo da VPC

O recurso VPC Flow Logs do Amazon VPC captura informações sobre o tráfego IP que entra e sai das interfaces de rede conectadas às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em seu ambiente. AWS

Quando você ativa GuardDuty, ele imediatamente começa a analisar seus registros de fluxo de VPC a partir de instâncias do Amazon EC2 em sua conta. Ele consome os eventos de VPC Flow Log diretamente do recurso de VPC Flow Logs por meio de um fluxo independente e duplicado de registros de fluxo. Esse processo não afeta nenhuma das suas configurações de log de fluxo existentes.

GuardDuty Proteção Lambda

A Proteção Lambda é um aprimoramento opcional da Amazon. GuardDuty Atualmente, o Monitoramento de atividades de rede do Lambda inclui registros de fluxo do Amazon VPC de todas as funções do Lambda para sua conta, mesmo aqueles que não usam redes VPC. Para proteger sua função Lambda de possíveis ameaças à segurança, você precisará configurar a Proteção Lambda em sua conta. GuardDuty Para ter mais informações, consulte GuardDuty Proteção Lambda.

GuardDuty Monitoramento de execução

Quando você gerencia o agente de segurança (manualmente ou por meio de GuardDuty) no EKS Runtime Monitoring ou Runtime Monitoring para instâncias EC2, e atualmente GuardDuty está implantado em uma instância Tipos de eventos de runtime coletados do Amazon EC2 e os recebe dessa instância, não GuardDuty cobrará pela análise dos registros de fluxo Conta da AWS de VPC dessa instância do Amazon EC2. Isso ajuda a GuardDuty evitar o dobro do custo de uso na conta.

GuardDuty não gerencia seus registros de fluxo nem os torna acessíveis em sua conta. Para gerenciar o acesso e a retenção dos seus registros de fluxo, você precisa configurar o recurso de Logs de fluxo da VPC.

Logs de DNS

Se você usar resolvedores de AWS DNS para suas instâncias do Amazon EC2 (a configuração padrão), GuardDuty poderá acessar e processar seus registros de DNS de solicitação e resposta por meio dos resolvedores de DNS internos. AWS Se você usar outro resolvedor de DNS, como OpenDNS ou GoogleDNS, ou se configurar seus próprios resolvedores GuardDuty de DNS, não poderá acessar e processar dados dessa fonte de dados.

Quando você ativa GuardDuty, ele começa imediatamente a analisar seus registros de DNS a partir de um fluxo independente de dados. Esse fluxo de dados é separado dos dados fornecidos pelo

atributo Registro em log de consultas do Resolvedor do Route 53. A configuração desse recurso não afeta a GuardDuty análise.

> **Note**
>
> GuardDuty não oferece suporte ao monitoramento de registros de DNS para instâncias do Amazon EC2 que são AWS Outposts iniciadas porque Amazon Route 53 Resolver o recurso de registro de consultas não está disponível nesse ambiente.

Proteção EKS na Amazon GuardDuty

O Monitoramento de logs de auditoria do EKS ajuda a detectar atividades potencialmente suspeitas em clusters do EKS no Amazon Elastic Kubernetes Service (Amazon EKS). O Monitoramento de logs de auditoria do EKS usa registros de auditoria do Kubernetes para capturar atividades cronológicas de usuários e aplicações usando a API Kubernetes e o ambiente de gerenciamento. Para ter mais informações, consulte Logs de auditoria do Kubernetes.

> **Note**
>
> O EKS Runtime Monitoring é gerenciado como parte do Runtime Monitoring. Para ter mais informações, consulte GuardDuty Monitoramento de execução.

Atributos da Proteção do EKS

Logs de auditoria do Kubernetes

Os logs de auditoria do Kubernetes capturam ações sequenciais em seu cluster do Amazon EKS, incluindo atividades de usuários e aplicações usando a API Kubernetes e o ambiente de gerenciamento. Os logs de auditoria são um componente de todos os clusters do Kubernetes.

Para obter mais informações, consulte Auditorias na documentação do Kubernetes.

O Amazon EKS permite que os registros de auditoria do Kubernetes sejam ingeridos como CloudWatch Amazon Logs por meio do recurso de registro do plano de controle do EKS. GuardDuty não gerencia o registro do plano de controle do Amazon EKS nem torna os registros de auditoria do Kubernetes acessíveis em sua conta se você não os tiver habilitado para o Amazon EKS. Para gerenciar o acesso e a retenção dos seus logs de auditoria do Kubernetes, você deve configurar o atributo de registro em log do ambiente de gerenciamento do Amazon EKS. Para obter mais informações, consulte Habilitar e desabilitar os logs do ambiente de gerenciamento no Guia do usuário da Amazon EKS.

Para obter informações sobre como configurar o Monitoramento de logs de auditoria do EKS, consulte Monitoramento de logs de auditoria do EKS.

Monitoramento de logs de auditoria do EKS

O Monitoramento de logs de auditoria do EKS ajuda você a detectar atividades potencialmente suspeitas em seus clusters do EKS no Amazon Elastic Kubernetes Service. Quando você ativa o EKS Audit Log Monitoring, GuardDuty imediatamente começa a monitorar seus clusters Logs de auditoria do Kubernetes do Amazon EKS e a analisá-los em busca de atividades potencialmente maliciosas e suspeitas. Ele consome eventos de log de auditoria do Kubernetes diretamente do recurso de registro do plano de controle do Amazon EKS por meio de um fluxo independente e duplicativo de registros de auditoria. Esse processo não exige nenhuma configuração adicional nem afeta nenhuma configuração existente de registro do ambiente de gerenciamento do Amazon EKS que você possa ter.

Quando você desativa o monitoramento do registro de auditoria do EKS, interrompe GuardDuty imediatamente o monitoramento e a análise dos registros de auditoria do Kubernetes para seus recursos do Amazon EKS.

O monitoramento do registro de auditoria do EKS pode não estar disponível em todos os Regiões da AWS locais GuardDuty disponíveis. Para ter mais informações, consulte Disponibilidade de recursos específicos da região.

Como o período de teste gratuito de 30 dias afeta as contas GuardDuty

- Quando você ativa GuardDuty pela primeira vez, o EKS Audit Log Monitoring no EKS Protection já está incluído no período de teste gratuito de 30 dias.
- As GuardDuty contas existentes podem ativar o EKS Audit Log Monitoring pela primeira vez com um período de teste gratuito de 30 dias.

Configuração do Monitoramento de logs de auditoria do EKS para uma conta independente

Escolha seu método de acesso preferido para habilitar ou desabilitar o Monitoramento de logs de auditoria do EKS para uma conta independente.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Proteção do EKS.

3. Na guia Configuração, você pode visualizar o status atual da configuração do Monitoramento de logs de auditoria do EKS. Na seção Monitoramento de logs de auditoria do EKS, escolha Habilitar para habilitar ou Desabilitar para desabilitar o recurso Monitoramento de logs de auditoria do EKS.
4. Selecione Salvar.

API/CLI

- Execute a operação da updateDetectorAPI usando o ID do detector regional da conta do GuardDuty administrador delegado e transmitindo o nome do `features` objeto como `EKS_AUDIT_LOGS` e o status como `ENABLED` ou`DISABLED`.

  Como alternativa, você também pode ativar ou desativar o EKS Audit Log Monitoring executando o AWS CLI comando a. O código de exemplo a seguir ativa o GuardDuty EKS Audit Log Monitoring. Para desabilitá-la, substitua `ENABLED` por `DISABLED`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  features [{"Name" : "EKS_AUDIT_LOGS", "Status" : "ENABLED"}]'
  ```

Configuração do Monitoramento de logs de auditoria do EKS para ambientes com várias contas

Em um ambiente de várias contas, somente a conta do GuardDuty administrador delegado tem a opção de ativar ou desativar o recurso EKS Audit Log Monitoring; para as contas dos membros em sua organização. As contas GuardDuty dos membros não podem modificar essa configuração em suas contas. A conta de GuardDuty administrador delegado gerencia suas contas de membros usando AWS Organizations. Essa conta de GuardDuty administrador delegado pode optar por habilitar automaticamente o EKS Audit Log Monitoring para todas as novas contas à medida que elas ingressam na organização. Para obter mais informações sobre ambientes com várias contas, consulte Gerenciamento de várias contas na Amazon. GuardDuty

Configurando o monitoramento do registro de auditoria do EKS para uma conta de administrador delegado GuardDuty

Escolha seu método de acesso preferido para configurar o EKS Audit Log Monitoring para a conta do GuardDuty administrador delegado.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de gerenciamento.
2. No painel de navegação, escolha Proteção do EKS.
3. Na guia Configuração, você pode visualizar o status atual da configuração do Monitoramento de logs de auditoria do EKS na seção respectiva. Para atualizar a configuração da conta de GuardDuty administrador delegado, escolha Editar no painel Monitoramento do log de auditoria do EKS.
4. Execute um destes procedimentos:

   Como usar a opção Habilitar para todas as contas

   - Escolha Habilitar para todas as contas. Isso habilitará o plano de proteção para todas as GuardDuty contas ativas em sua AWS organização, incluindo as novas contas que ingressam na organização.
   - Escolha Salvar.

   Como usar a opção Configurar contas manualmente

   - Para habilitar o plano de proteção somente para a conta de GuardDuty administrador delegado, escolha Configurar contas manualmente.
   - Escolha Habilitar na seção Conta de GuardDuty administrador delegado (esta conta).
   - Escolha Salvar.

API/CLI

Execute a operação da API updateDetector usando seu próprio ID de detector regional e transmitindo o `name` do objeto `features` como `EKS_AUDIT_LOGS` e `status` como `ENABLED` ou `DISABLED`.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

Você pode ativar ou desativar o EKS Audit Log Monitoring executando o seguinte AWS CLI comando. Certifique-se de usar o *`ID de detector`* válido da conta de GuardDuty administrador delegado.

> **Note**
>
> O código de exemplo a seguir habilita o Monitoramento de logs de auditoria do EKS. *`Certifique-se de substituir 12abc34d567e8fa901bc2d34e56789f0 pela conta do administrador delegado e 5555555555 pela conta do administrador delegado. detector-id GuardDuty`* Conta da AWS GuardDuty

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --accountids 555555555555 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
 "ENABLED"}]'
```

Para desabilitar o Monitoramento de logs de auditoria do EKS, substitua `ENABLED` por `DISABLED`.

Habilite automaticamente o Monitoramento de logs de auditoria do EKS para todas as contas-membro

Escolha seu método de acesso preferido para habilitar o Monitoramento de logs de auditoria do EKS para contas-membro existentes em sua organização.

Console

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

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. Execute um destes procedimentos:

Usando a página Proteção do EKS

1. No painel de navegação, escolha Proteção do EKS.
2. Na guia Configuração, você pode ver o status atual do Monitoramento de logs de auditoria do EKS para contas-membro ativas em sua organização.

   Para atualizar a configuração do Monitoramento de logs de auditoria do EKS, escolha Editar.
3. Escolha Habilitar para todas as contas. Essa ação habilita automaticamente o Monitoramento de logs de auditoria do EKS para as contas existentes e novas na organização.
4. Escolha Salvar.

> **Note**
>
> Pode levar até 24 horas para atualizar a configuração das contas-membro.

Como usar a página Contas

1. No painel de navegação, escolha Accounts (Contas).
2. Na página Contas, escolha Habilitar automaticamente as preferências antes de Adicionar contas por convite.
3. Na janela Gerenciar preferências de habilitação automática, escolha Habilitar para todas as contas em Monitoramento de logs de auditoria do EKS.
4. Escolha Salvar.

Se você não puder usar a opção Habilitar para todas as contas e quiser personalizar a configuração do Monitoramento de logs de auditoria do EKS para contas específicas em sua organização, consulte Habilitar ou desabilitar seletivamente o Monitoramento de logs de auditoria do EKS para contas-membro.

API/CLI

- Para habilitar ou desabilitar seletivamente o Monitoramento de logs de auditoria do EKS para suas contas-membro, execute a operação da API updateMemberDetectors usando seu próprio *ID de detector*.
- O exemplo a seguir mostra como você pode habilitar o Monitoramento de logs de auditoria do EKS para uma única conta-membro. Para desabilitá-la, substitua `ENABLED` por `DISABLED`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Você também pode passar uma lista de IDs de contas separadas por um espaço.

- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Habilite o Monitoramento de logs de auditoria do EKS para todas as contas-membro ativas existentes

Escolha seu método de acesso preferido para habilitar o Monitoramento de logs de auditoria do EKS para todas as contas-membro ativas existentes na organização.

Console

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

   Faça login usando as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, escolha Proteção do EKS.
3. Na página EKS Protection, você pode ver o status atual da configuração de verificação de GuardDuty malware iniciada. Na seção Contas-membro ativas, escolha Ações.
4. No menu suspenso Ações, escolha Habilitar para todas as contas-membro ativas existentes.

5. Escolha Salvar.

API/CLI

- Para habilitar ou desabilitar seletivamente o Monitoramento de logs de auditoria do EKS para suas contas-membro, execute a operação da API updateMemberDetectors usando seu próprio *ID de detector*.
- O exemplo a seguir mostra como você pode habilitar o Monitoramento de logs de auditoria do EKS para uma única conta-membro. Para desabilitá-la, substitua `ENABLED` por `DISABLED`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "EKS_AUDIT_LOGS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Você também pode passar uma lista de IDs de contas separadas por um espaço.

- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Habilite automaticamente o Monitoramento de logs de auditoria do EKS para novas contas-membro

As contas de membros recém-adicionadas devem ser ativadas GuardDuty antes de selecionar a configuração da verificação de GuardDuty malware iniciada. As contas dos membros gerenciadas por convite podem configurar manualmente a verificação de GuardDuty malware iniciada por suas contas. Para ter mais informações, consulte Step 3 - Accept an invitation.

Escolha seu método de acesso preferido para habilitar o Monitoramento de logs de auditoria do EKS para novas contas que ingressam na sua organização.

Console

A conta de GuardDuty administrador delegado pode ativar o Monitoramento do Registro de Auditoria do EKS para novas contas membros em uma organização, usando o Monitoramento do Registro de Auditoria do EKS ou a página Contas.

Para habilitar automaticamente o Monitoramento de logs de auditoria do EKS para novas contas-membro

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.

2. Execute um destes procedimentos:

   - Usando a página Proteção do EKS:

     1. No painel de navegação, escolha Proteção do EKS.
     2. Na página Proteção do EKS, escolha Editar no Monitoramento de logs de auditoria do EKS.
     3. Escolha Configurar contas manualmente.
     4. Selecione Habilitar automaticamente para novas contas-membro. Essa etapa garante que sempre que uma nova conta ingressar em sua organização, o Monitoramento de logs de auditoria do EKS seja habilitado automaticamente para sua conta. Somente a conta do GuardDuty administrador delegado da organização pode modificar essa configuração.
     5. Selecione Salvar.

   - Como usar a página Contas:

     1. No painel de navegação, escolha Accounts (Contas).
     2. Na página Contas, escolha Habilitar automaticamente as preferências.
     3. Na janela Gerenciar preferências de habilitação automática, selecione Habilitar para novas contas em Monitoramento de logs de auditoria do EKS.
     4. Escolha Salvar.

API/CLI

- Para habilitar ou desabilitar seletivamente o Monitoramento de logs de auditoria do EKS para suas novas contas, execute a operação da API UpdateOrganizationConfiguration usando seu próprio *ID de detector*.
- O exemplo a seguir mostra como você pode habilitar o Monitoramento de logs de auditoria do EKS para os novos membros que ingressarem na sua organização. Você também pode passar uma lista de IDs de contas separadas por um espaço.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
   "EKS_AUDIT_LOGS", "AutoEnable": "NEW"}]'
  ```

Habilitar ou desabilitar seletivamente o Monitoramento de logs de auditoria do EKS para contas-membro

Escolha seu método de acesso preferido para habilitar ou desabilitar o Monitoramento de logs de auditoria do EKS para contas-membro seletivas em sua organização.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, escolha Accounts (Contas).

   Na página Contas, revise a coluna Monitoramento de logs de auditoria do EKS para ver o status da sua conta-membro.
3. Para habilitar ou desabilitar o Monitoramento de logs de auditoria do EKS

   Selecione uma conta que você deseja configurar para o Monitoramento de logs de auditoria do EKS. Você pode selecionar várias contas ao mesmo tempo. No menu suspenso Editar planos de proteção, escolha Monitoramento de logs de auditoria do EKS e escolha a opção apropriada.

API/CLI

Para habilitar ou desabilitar seletivamente o Monitoramento de logs de auditoria do EKS para suas contas-membro, invoque a operação da API updateMemberDetectors usando seu próprio *ID de detector*.

O exemplo a seguir mostra como você pode habilitar o Monitoramento de logs de auditoria do EKS para uma única conta-membro. Para desabilitá-la, substitua `ENABLED` por `DISABLED`. Você também pode passar uma lista de IDs de contas separadas por um espaço.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --accountids 111122223333 --features '[{"Name": "EKS_AUDIT_LOGS", "Status":
 "ENABLED"}]'
```

Proteção Lambda na Amazon GuardDuty

A Proteção do Lambda ajuda você a identificar possíveis ameaças à segurança quando uma função do AWS Lambda é invocada em seu ambiente da AWS . Quando você ativa o Lambda Protection, GuardDuty começa a monitorar os registros de atividades da rede Lambda, começando com Logs de fluxo da VPC todas as funções do Lambda da conta, incluindo os registros que não usam redes VPC e são gerados quando a função Lambda é invocada. Se GuardDuty identificar tráfego de rede suspeito que seja indicativo da presença de um código potencialmente malicioso em sua função Lambda, GuardDuty gerará uma descoberta.

> **Note**
>
> O Monitoramento de atividades de rede do Lambda não inclui os registros das funções do Lambda@Edge.

Você pode configurar a Proteção Lambda para qualquer conta ou disponível Regiões da AWS, a qualquer momento. Por padrão, uma GuardDuty conta existente pode ativar a Proteção Lambda com um período de teste de 30 dias. Para uma nova GuardDuty conta, a Proteção Lambda já está ativada e incluída no período de teste de 30 dias. Para mais informações sobre estatísticas de uso, consulte Como estimar os custos.

GuardDuty monitora os registros de atividades de rede gerados pela invocação das funções Lambda. Atualmente, o Monitoramento de atividades de rede do Lambda inclui registros de fluxo do Amazon VPC de todas as funções do Lambda da sua conta, incluindo aqueles registros que não usam redes VPC e estão sujeitos a alterações, incluindo expansão para outras atividades de rede, como dados de consulta ao DNS gerados pela invocação das funções Lambda. A expansão para outras formas de monitoramento de atividades de rede aumentará o volume de dados que GuardDuty serão processados para a Proteção Lambda. Isso afetará diretamente o custo de uso da Proteção do Lambda. Sempre que GuardDuty começar a monitorar um registro adicional de atividades de rede, ele fornecerá um aviso às contas que ativaram a Proteção Lambda, pelo menos 30 dias antes do lançamento.

Recurso na Proteção do Lambda

Monitoramento de atividades da rede Lambda

Quando você ativa a Proteção Lambda, monitora os registros de atividades GuardDuty da rede Lambda gerados quando uma função Lambda associada à sua conta é invocada. Isso ajuda você a detectar possíveis ameaças à segurança da função Lambda. GuardDuty monitora os registros de fluxo de VPC de todas as suas funções do Lambda, incluindo aquelas que não usam redes VPC. Para funções do Lambda configuradas para usar redes VPC, você não precisa habilitar os registros de fluxo da VPC para as interfaces de rede elástica (ENI) criadas pelo Lambda para. GuardDuty GuardDuty cobra apenas pela quantidade de dados de registros de atividades da rede Lambda processados (em GB) para gerar uma descoberta. GuardDuty otimiza os custos aplicando filtros inteligentes e analisando um subconjunto dos registros de atividades da rede Lambda que são relevantes para a detecção de ameaças. Para obter informações sobre preços, consulte GuardDuty Preços da Amazon.

GuardDuty não gerencia seus registros de atividades da rede Lambda (incluindo registros de fluxo VPC e não VPC) nem os torna acessíveis em sua conta.

Como configurar a Proteção do Lambda

Configurando a Proteção do Lambda para uma conta independente

Para contas associadas à AWS Organizations, você pode automatizar esse processo por meio de instruções GuardDuty do console ou da API, conforme descrito na próxima seção.

Escolha seu método de acesso preferido para habilitar ou desabilitar a Proteção do Lambda para uma conta independente.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, em Configurações, escolha Proteção do Lambda.
3. A página Proteção do Lambda mostra o status atual da sua conta. Você pode habilitar ou desabilitar o recurso a qualquer momento selecionando Habilitar ou Desabilitar.
4. Escolha Salvar.

API/CLI

Execute a operação da API updateDetector usando seu próprio ID de detector regional e transmitindo o `name` do objeto `features` como `LAMBDA_NETWORK_LOGS` e `status` como `ENABLED` ou `DISABLED`.

Você também pode ativar ou desativar o Lambda Network Activity Monitoring executando o comando a seguir AWS CLI . Use seu próprio *`ID de detector`* válido.

> **Note**
>
> O código de exemplo a seguir habilita o Monitoramento de atividades de rede do Lambda. Para desabilitá-la, substitua `ENABLED` por `DISABLED`.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features [{"Name" : "LAMBDA_NETWORK_LOGS", "Status" : "ENABLED"}]'
```

Configurando a Proteção do Lambda em ambientes com várias contas

Em um ambiente com várias contas, somente a conta do GuardDuty administrador delegado tem a opção de ativar ou desativar a Proteção Lambda para as contas dos membros em sua organização. As contas GuardDuty dos membros não podem modificar essa configuração em suas contas. A conta de GuardDuty administrador delegado gerencia as contas dos membros usando AWS Organizations. A conta de GuardDuty administrador delegado pode optar por habilitar automaticamente o Lambda Network Activity Monitoring para todas as novas contas à medida que elas ingressam na organização. Para obter mais informações sobre ambientes com várias contas, consulte Gerenciamento de várias contas na Amazon GuardDuty.

Configurando a Proteção Lambda para uma conta de administrador delegado GuardDuty

Escolha seu método de acesso preferido para ativar ou desativar o Lambda Network Activity Monitoring para uma conta de administrador delegado GuardDuty .

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de gerenciamento.
2. No painel de navegação, em Configurações, escolha Proteção do Lambda.
3. Na página Proteção do Lambda, escolha Editar.
4. Execute um destes procedimentos:

   Como usar a opção Habilitar para todas as contas

   - Escolha Habilitar para todas as contas. Isso habilitará o plano de proteção para todas as GuardDuty contas ativas em sua AWS organização, incluindo as novas contas que ingressam na organização.
   - Escolha Salvar.

   Como usar a opção Configurar contas manualmente

   - Para ativar o plano de proteção somente para a conta de GuardDuty administrador delegado, escolha Configurar contas manualmente.
   - Escolha Habilitar na seção Conta de GuardDuty administrador delegado (esta conta).
   - Escolha Salvar.

API/CLI

Execute a operação da API updateDetector usando seu próprio ID de detector regional e transmitindo o `name` do objeto `features` como `LAMBDA_NETWORK_LOGS` e `status` como `ENABLED` ou `DISABLED`.

Você pode ativar ou desativar o Lambda Network Activity Monitoring executando o comando a seguir AWS CLI . Certifique-se de usar o *`ID de detector`* válido da conta de GuardDuty administrador delegado.

> **Note**
>
> O código de exemplo a seguir habilita o Monitoramento de atividades de rede do Lambda. Para desabilitá-la, substitua `ENABLED` por `DISABLED`.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-ids 555555555555 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status":
 "ENABLED"}]'
```

Habilite automaticamente o monitoramento de atividades da rede Lambda para todas as contas-membro

Escolha seu método de acesso preferido para habilitar o recurso Monitoramento de atividades de rede do Lambda para todas as contas-membro. Isso inclui contas-membro existentes e as novas contas que ingressam na organização.

Console

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

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. Execute um destes procedimentos:

   Usando a página de Proteção do Lambda

   1. No painel de navegação, escolha Proteção do Lambda.
   2. Escolha Habilitar para todas as contas. Essa ação habilita automaticamente o Monitoramento de atividades de rede do Lambda para contas existentes e novas na organização.
   3. Escolha Salvar.

      > **Note**
      >
      > Pode levar até 24 horas para atualizar a configuração das contas-membro.

   Como usar a página Contas

   1. No painel de navegação, escolha Accounts (Contas).

2. Na página Contas, escolha Habilitar automaticamente as preferências antes de Adicionar contas por convite.
3. Na janela Gerenciar preferências de habilitação automática, escolha Habilitar para todas as contas em Monitoramento de atividades de rede do Lambda.

> **Note**
>
> Por padrão, essa ação ativa automaticamente a opção Ativar automaticamente GuardDuty para novas contas de membros.

4. Escolha Salvar.

Se você não conseguir usar a opção Habilitar para todas as contas, consulte Habilite ou desabilite seletivamente o Monitoramento de atividades de rede do Lambda para contas-membro.

API/CLI

- Para habilitar ou desabilitar seletivamente o Monitoramento de atividades de rede do Lambda para suas contas-membro, invoque a operação da API updateMemberDetectors usando seu próprio *ID de detector*.
- O exemplo a seguir mostra como você pode habilitar o Monitoramento de atividades de rede do Lambda para uma única conta de membro. Para desabilitar uma conta de membro, substitua `ENABLED` por `DISABLED`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
  ```

  Você também pode passar uma lista de IDs de contas separadas por um espaço.
- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Habilite o monitoramento de atividades da rede Lambda para todas as contas-membro ativas existentes

Escolha seu método de acesso preferido para habilitar o Monitoramento de atividades de rede do Lambda para todas as contas-membro ativas existentes na organização.

Console

Para configurar o Monitoramento de atividades de rede do Lambda para todas as contas-membro ativas existentes

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

   Faça login usando as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, escolha Proteção do Lambda.
3. Na página Proteção do Lambda, você pode visualizar o status atual da configuração. Na seção Contas-membro ativas, escolha Ações.
4. No menu suspenso Ações, escolha Habilitar para todas as contas-membro ativas existentes.
5. Selecione a opção Confirmar.

API/CLI

- Para habilitar ou desabilitar seletivamente o Monitoramento de atividades de rede do Lambda para suas contas-membro, invoque a operação da API updateMemberDetectors usando seu próprio *ID de detector*.
- O exemplo a seguir mostra como você pode habilitar o Monitoramento de atividades de rede do Lambda para uma única conta de membro. Para desabilitar uma conta de membro, substitua `ENABLED` por `DISABLED`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"Name": "LAMBDA_NETWORK_LOGS", "Status": "ENABLED"}]'
  ```

  Você também pode passar uma lista de IDs de contas separadas por um espaço.

- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Habilite automaticamente o monitoramento de atividades da rede Lambda para novas contas-membro

Escolha seu método de acesso preferido para habilitar o Monitoramento de atividades de rede do Lambda para novas contas que ingressam na sua organização.

Console

A conta de GuardDuty administrador delegado pode habilitar o Lambda Network Activity Monitoring para novas contas de membros em uma organização, usando a página Lambda Protection ou Accounts.

Para habilitar automaticamente o Monitoramento de atividades de rede do Lambda para novas contas-membro

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. Execute um destes procedimentos:
   - Usando a página de Proteção do Lambda:
     1. No painel de navegação, escolha Proteção do Lambda.
     2. Na página Proteção do Lambda, escolha Editar.
     3. Escolha Configurar contas manualmente.
     4. Selecione Habilitar automaticamente para novas contas-membro. Essa etapa garante que sempre que uma nova conta ingressar na sua organização, a Proteção do Lambda seja habilitada automaticamente para a conta dessa pessoa. Somente a conta do GuardDuty administrador delegado da organização pode modificar essa configuração.
     5. Selecione Salvar.
   - Como usar a página Contas:
     1. No painel de navegação, escolha Accounts (Contas).

2. Na página Contas, escolha Habilitar automaticamente as preferências.
3. Na janela Gerenciar preferências de habilitação automática, selecione Habilitar para novas contas em Monitoramento de atividades de rede do Lambda.
4. Escolha Salvar.

API/CLI

- Para habilitar ou desabilitar o Monitoramento de atividades de rede do Lambda para novas contas-membro, invoque a operação da API UpdateOrganizationConfiguration usando seu próprio *ID de detector*.
- O exemplo a seguir mostra como você pode habilitar o Monitoramento de atividades de rede do Lambda para uma única conta de membro. Para desabilitá-lo, consulte Habilite ou desabilite seletivamente o Monitoramento de atividades de rede do Lambda para contas-membro. Se não quiser habilitá-lo para todas as novas contas que ingressarem na organização, defina `AutoEnable` como `NONE`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
   "LAMBDA_NETWORK_LOGS", "AutoEnable": "NEW"}]'
  ```

  Você também pode passar uma lista de IDs de contas separadas por um espaço.
- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Habilite ou desabilite seletivamente o Monitoramento de atividades de rede do Lambda para contas-membro

Escolha seu método de acesso preferido para habilitar ou desabilitar seletivamente o Monitoramento de atividades de rede do Lambda para contas-membro.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.

2. No painel de navegação, em Settings, selecione Accounts.

   Na página Contas, revise a coluna Monitoramento de atividades de rede do Lambda. Ele indica se o Monitoramento de atividades de rede do Lambda está habilitado ou não.

3. Escolha a conta para a qual deseja configurar a Proteção do Lambda. É possível escolher várias contas ao mesmo tempo.
4. No menu suspenso Editar planos de proteção, escolha Monitoramento de atividades de rede do Lambda e escolha uma ação apropriada.

API/CLI

Invoque a API updateMemberDetectors usando seu próprio *`ID de detector`*.

O exemplo a seguir mostra como você pode habilitar o Monitoramento de atividades de rede do Lambda para uma única conta de membro. Para desabilitá-la, substitua `ENABLED` por `DISABLED`.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "LAMBDA_NETWORK_LOGS", "Status":
 "ENABLED"}]'
```

Você também pode passar uma lista de IDs de contas separadas por um espaço.

Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Proteção contra malware na Amazon GuardDuty

A Proteção contra malware ajuda você a detectar a presença de malware ao examinar os volumes do Amazon Elastic Block Store (Amazon EBS) que são anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e workloads de contêiner. A Proteção contra malware fornece opções de verificação nas quais você pode decidir se deseja incluir ou excluir instâncias específicas do Amazon EC2 e workloads de contêineres no momento da verificação. Ele também oferece a opção de reter os snapshots dos volumes do Amazon EBS anexados às instâncias do Amazon EC2 ou às cargas de trabalho de contêineres em suas contas. GuardDuty Os snapshots são retidos somente quando o malware é encontrado e as descobertas da Proteção contra malware são geradas.

O Malware Protection oferece dois tipos de escaneamento para detectar atividades potencialmente maliciosas em suas instâncias e cargas de trabalho de contêineres do Amazon EC2 GuardDuty: escaneamento de malware iniciado e escaneamento de malware sob demanda. A tabela a seguir mostra a comparação entre os dois tipos de verificação.

Factor	GuardDuty- verificação de malware iniciada	Verificação de malware sob demanda
Como a verificação é invocada	Depois de ativar a verificação de GuardDuty malware iniciada, sempre que GuardDuty gerar uma descoberta que indique a presença potencial de malware em uma instância do Amazon EC2 ou em uma carga de trabalho de contêiner GuardDuty , inicia automaticamente uma verificação de malware sem agente nos volumes do Amazon EBS anexados ao seu recurso potencialmente afetado. Para ter mais informações, consulte	Você pode iniciar uma verificação de malware sob demanda fornecendo o nome do recurso da Amazon (ARN) associado à sua instância do Amazon EC2 ou workload do contêiner. Você pode iniciar uma verificação de malware sob demanda mesmo quando nenhuma GuardDuty descoberta for gerada para seu recurso. Para ter mais informações, consulte Verificação de malware sob demanda.

Factor	GuardDuty- verificação de malware iniciada	Verificação de malware sob demanda
	GuardDuty- verificação de malware iniciada.	
Configuração necessária	Para usar a verificação GuardDuty de malware iniciada, você deve habilitá-la para sua conta. Para ter mais informações, consulte Configurando a verificação de GuardDuty malware iniciada.	Sua conta deve estar GuardDuty ativada. Para usar a verificação de malware sob demanda, não há necessida de de configuração no nível do recurso.
Tempo de espera para iniciar uma nova verificação	Sempre que GuardDuty gera um delesDescobertas que invocam uma verificação GuardDuty de malware iniciada, uma verificação de malware é iniciada automatic amente apenas uma vez a cada 24 horas.	Você pode iniciar uma verificação de malware sob demanda no mesmo recurso a qualquer momento após 1 hora a partir da hora de início da verificação anterior.
Disponibilidade do período de teste gratuito de 30 dias	Ao ativar a verificação GuardDuty de malware iniciada pela primeira vez em sua conta, você pode usar um período de teste gratuito de 30 dias*.	Não há período de teste gratuito* com a verificação de malware sob demanda para GuardDuty contas novas ou existentes.

Factor	GuardDuty- verificação de malware iniciada	Verificação de malware sob demanda
Opções de verificação	Depois de configurar a verificação de GuardDuty malware iniciada, a Proteção contra Malware também ajuda você a selecionar quais recursos devem ser verificados ou ignorados. A Proteção contra malware não iniciará uma verificação automática dos recursos que você optar por excluir da verificação.	A verificação de malware sob demanda oferece suporte a uma tag global —`GuardDuty Excluded` . Opções de verificação com tags definidas pelo usuárionão se aplica à verificação de malware sob demanda porque você fornece o ARN do recurso manualmente.

*Você incorrerá em custos de uso para criar snapshots de volumes do EBS e reter snapshots. Para obter mais informações sobre como configurar sua conta para reter instantâneos, consulte. Retenção de snapshots

A proteção contra malware é um aprimoramento opcional e foi projetada de forma a não afetar o desempenho de seus recursos. GuardDuty Para obter informações sobre como a Proteção contra Malware funciona GuardDuty, consulteAtributo na Proteção contra malware. Para obter informações sobre a disponibilidade da Proteção contra Malware em diferentes Regiões da AWS, consulteRegiões e endpoints.

> **Note**
>
> GuardDuty A Proteção contra Malware não é compatível com o Fargate nem com o Amazon EKS nem com o Amazon ECS.

Atributo na Proteção contra malware

Volume do Elastic Block Storage (EBS)

Esta seção explica como a proteção contra malware, incluindo a verificação de GuardDuty malware iniciada e a verificação de malware sob demanda, verifica os volumes do Amazon EBS associados

às suas instâncias e cargas de trabalho de contêineres do Amazon EC2. Antes de continuar, considere as seguintes personalizações:

- Opções de verificação: a Proteção contra malware oferece a capacidade de especificar tags para incluir ou excluir instâncias do Amazon EC2 e volumes do Amazon EBS do processo de verificação. Somente a verificação GuardDuty de malware iniciada oferece suporte às opções de verificação com tags definidas pelo usuário. Tanto a verificação GuardDuty de malware iniciada quanto a verificação de malware sob demanda oferecem suporte à tag global`GuardDutyExcluded`. Para ter mais informações, consulte Opções de verificação com tags definidas pelo usuário.
- Retenção de snapshots — A proteção contra malware oferece uma opção para reter os snapshots dos volumes do Amazon EBS em sua conta. AWS Esta opção está desabilitada por padrão. Você pode optar pela retenção de instantâneos para escaneamentos de malware GuardDuty iniciados e sob demanda. Para ter mais informações, consulte Retenção de snapshots.

Quando GuardDuty gera uma descoberta indicativa da possível presença de malware em uma instância do Amazon EC2 ou em uma carga de trabalho de contêiner e você habilita GuardDuty o tipo de verificação iniciada no Malware Protection, GuardDuty uma verificação de malware iniciada pode ser invocada com base em suas opções de verificação.

Para iniciar uma verificação de malware sob demanda nos volumes do Amazon EBS associados a uma instância do Amazon EC2, forneça o nome do recurso da Amazon (ARN) da instância do Amazon EC2.

Como resposta a uma verificação de malware sob demanda ou a uma verificação de GuardDuty malware iniciada automaticamente, GuardDuty cria instantâneos dos volumes relevantes do EBS anexados ao recurso potencialmente afetado e os compartilha com o. GuardDuty conta de serviço A partir desses instantâneos, GuardDuty cria uma réplica criptografada do volume do EBS na conta de serviço.

Após a conclusão da verificação, GuardDuty exclui os volumes de réplica criptografados do EBS e os instantâneos dos seus volumes do EBS. Se um malware for encontrado e você tiver ativado a configuração de retenção de instantâneos, os instantâneos dos seus volumes do EBS não serão excluídos e serão automaticamente retidos em sua conta. AWS Quando nenhum malware for encontrado, os snapshots dos seus volumes do EBS não serão retidos, independentemente da configuração de retenção de snapshots. Como padrão, a configuração de retenção de snapshots permanece desabilitada. Para obter informações sobre os custos dos snapshots e sua retenção, consulte os preços do Amazon EBS.

GuardDuty reterá cada volume de réplica do EBS na conta de serviço por até 55 horas. Se houver uma interrupção ou falha no serviço com uma réplica do volume do EBS e sua verificação de malware, esse volume do EBS GuardDuty será retido por no máximo sete dias. O período estendido de retenção de volume serve para fazer a triagem e resolver a interrupção ou falha. GuardDuty A Proteção contra Malware excluirá os volumes de réplica do EBS da conta de serviço após a interrupção ou falha ser resolvida, ou quando o período de retenção estendido expirar.

Volumes do Amazon EBS compatíveis para verificação de malware

Em todos os Regiões da AWS locais onde há GuardDuty suporte ao recurso de proteção contra malware, você pode escanear os volumes do Amazon EBS que não estão criptografados ou não estão criptografados. Você pode ter volumes do Amazon EBS criptografados com uma Chave gerenciada pela AWSou com a chave gerenciada pelo cliente. Atualmente, alguns Regiões da AWS oferecem suporte às duas formas de criptografar seus volumes do Amazon EBS, enquanto outros oferecem suporte apenas à chave gerenciada pelo cliente.

Para obter mais informações em que esse recurso ainda não é suportado, consulte China Regions

A lista a seguir descreve a chave que GuardDuty usa se seus volumes do Amazon EBS estão criptografados ou não:

- Volumes do Amazon EBS que não são criptografados ou criptografados com Chave gerenciada pela AWS — GuardDuty usam sua própria chave para criptografar os volumes de réplica do Amazon EBS.

  Quando sua conta pertence a uma Região da AWS que não suporta a digitalização de volumes do Amazon EBS que são criptografados com o padrão Chave gerenciada pela AWS para o EBS, consulte. Modificando o ID da AWS KMS chave padrão de um volume do Amazon EBS
- Volumes do Amazon EBS que são criptografados com chave gerenciada pelo cliente — GuardDuty usam a mesma chave para criptografar o volume de réplica do EBS.

A proteção contra malware não oferece suporte à verificação de instâncias do Amazon EC2 com `productCode` as. `marketplace` Se uma verificação de malware for iniciada para essa instância do Amazon EC2, a verificação será ignorada. Para obter mais informações, consulte `UNSUPPORTED_PRODUCT_CODE_TYPE` em Razões para ignorar o recurso durante a verificação de malware.

Modificando o ID da AWS KMS chave padrão de um volume do Amazon EBS

Por padrão, invocar a CreateVolumeAPI com criptografia definida como `true` e não especificar o ID da chave KMS cria um volume Amazon EBS que é criptografado com a AWS KMS chave padrão para criptografia do EBS. No entanto, quando uma chave de criptografia não é fornecida explicitamente, você pode modificar a chave padrão invocando a ModifyEbsDefaultKmsKeyIdAPI ou usando o comando correspondente AWS CLI .

Para modificar o ID da chave padrão do EBS, adicione a seguinte permissão necessária à sua política do IAM: `ec2:modifyEbsDefaultKmsKeyId`. Qualquer volume recém-criado do Amazon EBS que você escolher para ser criptografado, mas não especificar uma ID de chave KMS associada, usará a ID de chave padrão. Use um dos métodos a seguir para atualizar a ID da chave padrão do EBS:

Para modificar o ID da chave do KMS padrão de um volume do Amazon EBS

Execute um destes procedimentos:

- Usando uma API — Você pode usar a ModifyEbsDefaultKmsKeyIdAPI. Para obter informações sobre como você pode visualizar o status de criptografia do seu volume, consulte Criar volume do Amazon EBS.
- Usando o AWS CLI comando — O exemplo a seguir modifica a ID da chave KMS padrão que criptografará os volumes do Amazon EBS se você não fornecer uma ID da chave KMS. Certifique-se de substituir a região pela ID Região da AWS da sua chave KM.

  ```
  aws ec2 modify-ebs-default-kms-key-id --region us-west-2 --kms-key-
  id AKIAIOSFODNN7EXAMPLE
  ```

  O comando acima gerará uma saída semelhante à seguinte saída:

  ```
  {
    "KmsKeyId": "arn:aws:kms:us-west-2:444455556666:key/AKIAIOSFODNN7EXAMPLE"
  }
  ```

  Para obter mais informações, consulte modify-ebs-default-kms-key-id.

Personalizações na Proteção contra malware

Esta seção descreve como você pode personalizar as opções de varredura para suas instâncias do Amazon EC2 ou cargas de trabalho de contêineres quando uma verificação de malware é invocada, iniciada sob demanda ou por meio dela. GuardDuty

Configurações gerais

Retenção de snapshots

GuardDuty oferece a opção de reter os instantâneos dos volumes do EBS em sua AWS conta. Como padrão, a configuração de retenção de snapshots permanece desabilitada. Os snapshots só serão retidos se você tiver essa configuração habilitada antes do início da verificação.

Quando a verificação é iniciada, GuardDuty gera os volumes de réplica do EBS com base nos instantâneos dos seus volumes do EBS. Depois que a verificação for concluída e a configuração de retenção de snapshots em sua conta já estiver habilitada, os snapshots dos seus volumes do EBS serão retidos somente quando o malware for encontrado e as Tipos de descoberta de Malware Protection forem geradas. Independentemente de você ter ativado ou não a configuração de retenção de instantâneos, quando nenhum malware for detectado, GuardDuty excluirá automaticamente os instantâneos dos seus volumes do EBS.

Custo de uso de snapshots

Durante a verificação de malware, à medida que GuardDuty cria os snapshots dos seus volumes do Amazon EBS, há um custo de uso associado a essa etapa. Se você habilitar a configuração de retenção de snapshots em sua conta, quando o malware for encontrado e os snapshots forem retidos, você incorrerá no custo de uso do mesmo. Para obter informações sobre o custo dos snapshots e sua retenção, consulte os preços do Amazon EBS.

Escolha seu método de acesso preferido para habilitar a configuração de retenção de snapshots.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, em Planos de proteção, escolha Proteção contra malware.
3. Selecione Configurações gerais na seção inferior do console. Para reter os snapshots, ative a Retenção de snapshots.

API/CLI

1. Execute UpdateMalwareScanSettingspara atualizar a configuração atual da configuração de retenção de instantâneos.
2. Como alternativa, você pode executar o AWS CLI comando a seguir para reter automaticamente os instantâneos quando a Proteção contra GuardDuty Malware gerar descobertas.

   Certifique-se de substituir o *detector-id* pelo seu próprio `detectorId` válido.
3. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

   ```
   aws guardduty update-malware-scan-settings --detector-
   id 60b87779336485625 54d637e0e4bb3b2 --ebs-snapshot-preservation
    "RETENTION_WITH_FINDING"
   ```
4. Se você quiser desabilitar a retenção de snapshots, substitua `RETENTION_WITH_FINDING` por `NO_RETENTION`.

Opções de verificação com tags definidas pelo usuário

Ao usar a verificação de GuardDuty malware iniciada, você também pode especificar tags para incluir ou excluir instâncias do Amazon EC2 e volumes do Amazon EBS do processo de verificação e detecção de ameaças. Você pode personalizar cada escaneamento de GuardDuty malware iniciado editando as tags na lista de tags de inclusão ou exclusão. Cada lista pode incluir até 50 tags.

Se você ainda não tem tags definidas pelo usuário associadas aos seus recursos do EC2, consulte Marcar seus recursos do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias Linux ou Marcar seus recursos do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias do Windows.

> **Note**
>
> A verificação de malware sob demanda não oferece suporte a opções de verificação com tags definidas pelo usuário. Ele oferece suporte à Tag `GuardDutyExcluded` global.

Para excluir instâncias do EC2 da verificação de malware

Se você quiser excluir qualquer instância do Amazon EC2 ou volume do Amazon EBS durante o processo de digitalização, você pode definir a `GuardDutyExcluded` tag `true` para qualquer instância do Amazon EC2 ou volume do Amazon EBS e não a digitalizará. GuardDuty Para obter mais informações sobre a tag `GuardDutyExcluded`, consulte Permissões de função vinculada ao serviço para Proteção contra malware. Também é possível pode adicionar uma tag de instância do Amazon EC2 a uma lista de exclusão. Se você adicionar várias tags à lista de tags de exclusão, qualquer instância do Amazon EC2 que contenha pelo menos uma dessas tags será excluída do processo de verificação de malware.

Selecione seu método de acesso preferido para adicionar uma tag associada a uma instância do Amazon EC2 a uma lista de exclusão.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, em Planos de proteção, escolha Proteção contra malware.
3. Expanda a seção Tags de inclusão/exclusão. Selecione Adicionar tags.
4. Selecione Tags de exclusão e, em seguida, selecione Confirmar.
5. Especifique o par de **`Key`**-**`Value`** da tag que você deseja excluir. É opcional fornecer o **`Value`**. Depois de adicionar todas as tags, escolha Salvar.

   > **Important**
   >
   > As chaves e os valores de tags diferenciam maiúsculas de minúsculas. Para obter mais informações, consulte Restrições de tags no Guia do usuário do Amazon EC2 para instâncias do Linux ou Restrições de tags no Guia do usuário do Amazon EC2 para instâncias do Windows.

   Se um valor para uma chave não for fornecido e a instância do EC2 for marcada com a chave especificada, essa instância do EC2 será excluída do processo GuardDuty de verificação de malware iniciado, independentemente do valor atribuído à tag.

API/CLI

- Atualize as configurações de verificação de malware excluindo uma instância do EC2 ou uma workload de contêiner do processo de verificação.

  O comando de AWS CLI exemplo a seguir adiciona uma nova tag à lista de tags de exclusão. Certifique-se de substituir o *detector-id* de exemplo pelo seu próprio `detectorId` válido.

  `MapEquals` é uma lista de pares de `Key`/`Value`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --scan-resource-criteria '{"Exclude":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
 "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

  > **Important**
  >
  > As chaves e os valores de tags diferenciam maiúsculas de minúsculas. Para obter mais informações, consulte Restrições de tags no Guia do usuário do Amazon EC2 para instâncias do Linux ou Restrições de tags no Guia do usuário do Amazon EC2 para instâncias do Windows.

Para incluir instâncias do EC2 na verificação de malware

Se quiser verificar uma instância do EC2, adicione sua tag à lista de inclusão. Ao adicionar uma tag a uma lista de tags de inclusão, uma instância do EC2 que não contém nenhuma das tags adicionadas é ignorada na verificação de malware. Se você adicionar várias tags à lista de tags de inclusão, uma instância do EC2 que contenha pelo menos uma dessas tags será incluída na verificação de malware. Às vezes, uma instância do EC2 pode ser ignorada durante o processo de verificação. Para ter mais informações, consulte Razões para ignorar o recurso durante a verificação de malware.

Escolha seu método de acesso preferido para adicionar uma tag associada a uma instância do Amazon EC2 a uma lista de exclusão.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, em Planos de proteção, escolha Proteção contra malware.
3. Expanda a seção Tags de inclusão/exclusão. Selecione Adicionar tags.
4. Escolha Tags de inclusão e, em seguida, Confirmar.
5. Escolha Adicionar nova tag de inclusão e especifique o par de **`Key`**-**`Value`** que deseja incluir. É opcional fornecer o **`Value`**.

   Depois de adicionar todas as tags de inclusão, escolha Salvar.

   Se o valor de uma chave não for fornecido e uma instância do EC2 for marcada com a chave especificada, a instância do EC2 será incluída no processo de verificação da Proteção contra malware, independentemente do valor atribuído à tag.

API/CLI

- Atualize as configurações de verificação de malware para incluir uma instância do EC2 ou uma workload de contêiner no processo de verificação.

  O comando de AWS CLI exemplo a seguir adiciona uma nova tag à lista de tags de inclusão. Certifique-se de substituir o *`detector-id`* de exemplo pelo seu próprio `detectorId` válido. Substitua o exemplo *`TestKey`*e *`TestValue`*pelo `Value` par `Key` e da tag associada ao seu recurso do EC2.

  `MapEquals` é uma lista de pares de `Key`/`Value`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-malware-scan-settings --detector-
id 60b87779336485625 54d637e0e4bb3b2 --scan-resource-criteria '{"Include":
 {"EC2_INSTANCE_TAG" : {"MapEquals": [{ "Key": "TestKeyWithValue", "Value":
 "TestValue" }, {"Key":"TestKeyWithoutValue"} ]}}}' --ebs-snapshot-preservation
 "RETENTION_WITH_FINDING"
```

> **Important**
>
> As chaves e os valores de tags diferenciam maiúsculas de minúsculas. Para obter mais informações, consulte Restrições de tags no Guia do usuário do Amazon EC2 para instâncias do Linux ou Restrições de tags no Guia do usuário do Amazon EC2 para instâncias do Windows.

> **Note**
>
> Pode levar até 5 minutos GuardDuty para detectar uma nova etiqueta.

A qualquer momento, você pode escolher tags de inclusão ou tags de exclusão, mas não ambas. Se quiser alternar entre as tags, escolha essa tag no menu suspenso ao adicionar novas tags e Confirme sua seleção. Essa ação limpa todas as suas tags atuais.

Tag **`GuardDutyExcluded`** global

Por padrão, os snapshots dos seus volumes do EBS são criados com uma tag `GuardDutyScanId`. Não remova essa tag, pois isso GuardDuty impedirá o acesso aos instantâneos. Ambos os tipos de varredura na Proteção contra malware não examinam as instâncias do Amazon EC2 ou os volumes do Amazon EBS que têm a tag `GuardDutyExcluded` definida como `true`. Se a Proteção contra malware fizer uma verificação em tal recurso, um ID de verificação será gerado, mas a verificação será ignorada com o motivo `EXCLUDED_BY_SCAN_SETTINGS`. Para ter mais informações, consulte Razões para ignorar o recurso durante a verificação de malware.

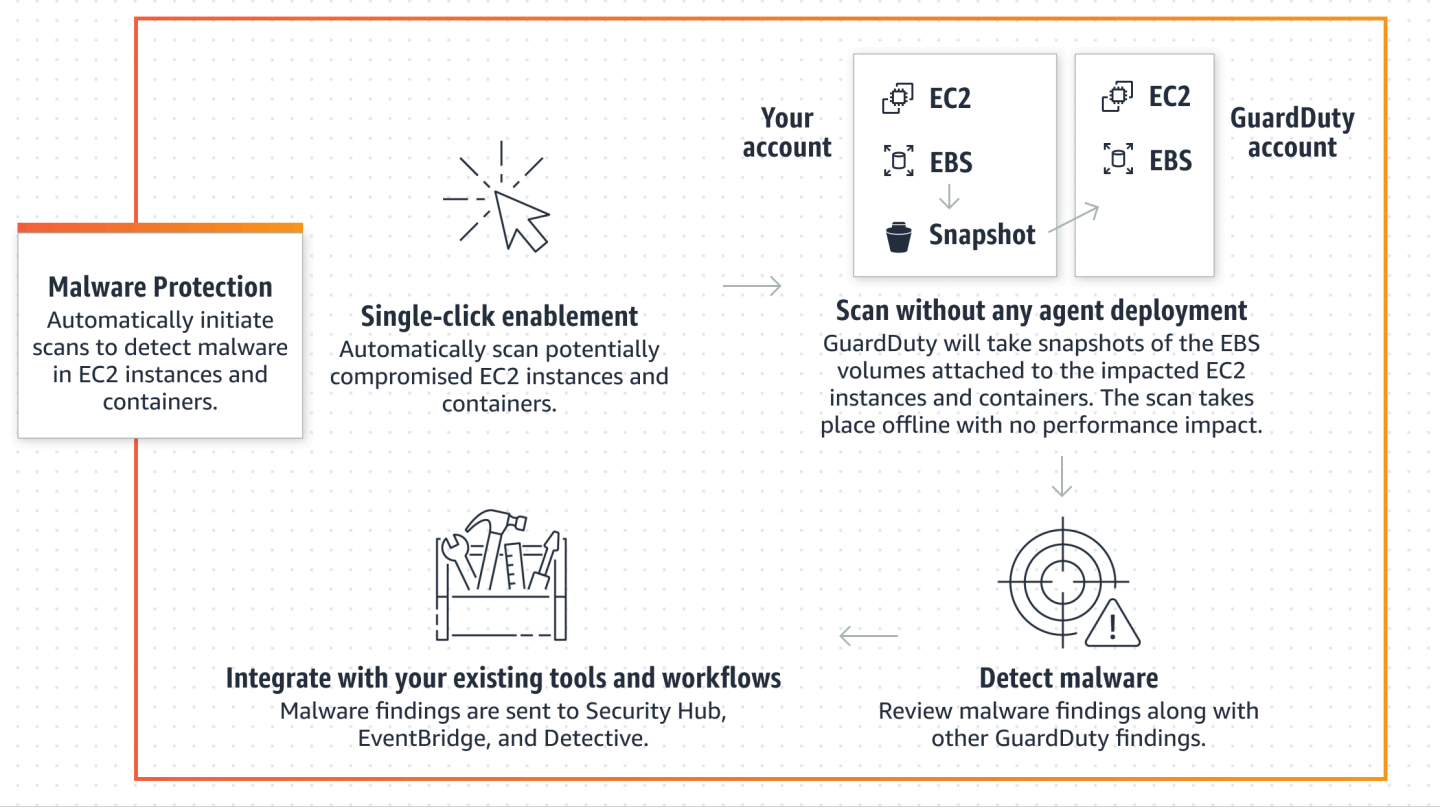
GuardDuty- verificação de malware iniciada

Com a verificação de GuardDuty malware iniciada ativada, sempre que GuardDuty detecta uma atividade maliciosa que indica a presença potencial de malware em sua instância ou carga de trabalho de contêiner do Amazon EC2 GuardDuty e Descobertas que invocam uma verificação GuardDuty de malware iniciada gera GuardDuty , inicia automaticamente uma verificação sem agente nos volumes do Amazon Elastic Block Store (Amazon EBS) anexados à instância do Amazon EC2 potencialmente afetada ou à carga de trabalho do contêiner para detectar a presença de malware. Com as opções de verificação, você pode adicionar tags de inclusão associadas aos

recursos que você deseja verificar ou adicionar tags de exclusão associadas aos recursos que você deseja ignorar no processo de verificação. O início automático da verificação sempre considerará suas opções de verificação. Você também pode optar por habilitar a configuração de retenção de snapshots para reter os snapshots de seus volumes do EBS somente se a Proteção contra malware detectar a presença de malware. Para ter mais informações, consulte Personalizações na Proteção contra malware.

Para cada instância do Amazon EC2 e carga de trabalho de contêiner que GuardDuty gera descobertas, uma verificação automática de malware GuardDuty iniciada é invocada uma vez a cada 24 horas. Para obter informações sobre como os volumes do Amazon EBS anexados à sua instância do Amazon EC2 ou workload do contêiner são verificados, consulte Atributo na Proteção contra malware.

A imagem a seguir descreve como a verificação GuardDuty de malware iniciada funciona.



Quando o malware é encontrado, é GuardDuty geradoTipos de descoberta de Malware Protection. Se GuardDuty não gerar uma descoberta indicativa de malware no mesmo recurso, nenhuma verificação de malware GuardDuty iniciada será invocada. Também é possível iniciar uma verificação de malware sob demanda no mesmo recurso. Para ter mais informações, consulte Verificação de malware sob demanda.

Como o período de teste gratuito de 30 dias afeta as contas GuardDuty

Você pode optar por ativar ou desativar a funcionalidade de verificação de GuardDuty malware iniciada para qualquer conta ou disponível Regiões da AWS, a qualquer momento.

- Quando você ativa GuardDuty pela primeira vez (nova GuardDuty conta), a verificação de GuardDuty malware iniciada já está ativada e incluída no período de teste gratuito de 30 dias.
- As GuardDuty contas existentes podem ativar a verificação GuardDuty de malware iniciada pela primeira vez com um período de teste gratuito de 30 dias.
- Se você já tem uma GuardDuty conta que estava usando a Proteção contra Malware antes da disponibilização geral da verificação de malware sob demanda e essa GuardDuty conta já usa o modelo de preços para ela Região da AWS, nenhuma ação é necessária para continuar usando a verificação de GuardDuty malware iniciada.

> **Note**
>
> Se você estiver em um período de teste gratuito de 30 dias, o custo de uso para criar os snapshots de volume do Amazon EBS e sua retenção ainda serão aplicados. Para obter mais informações, consulte Definição de preço do Amazon EBS.

Para obter informações sobre como ativar a verificação GuardDuty de malware iniciada, consulteConfigurando a verificação de GuardDuty malware iniciada.

Configurando a verificação de GuardDuty malware iniciada

Configurando a verificação GuardDuty de malware iniciada para uma conta independente

Para contas associadas a AWS Organizations, você pode automatizar esse processo por meio das configurações do console, conforme descrito na próxima seção.

Para ativar ou desativar a verificação GuardDuty de malware iniciada

Escolha seu método de acesso preferido para configurar a verificação de GuardDuty malware iniciada para uma conta independente.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, em Planos de proteção, escolha Proteção contra malware.
3. O painel Proteção contra malware lista o status atual da verificação de GuardDuty malware iniciada em sua conta. Você pode habilitá-la ou desabilitá-la a qualquer momento selecionando Habilitar ou Desabilitar, respectivamente.
4. Escolha Salvar.

API/CLI

- Execute a operação da API updateDetector usando seu próprio ID de detector regional e transmitindo o objeto `dataSources` com `EbsVolumes` definido como `true` ou `false`.

  Você também pode ativar ou desativar a verificação de GuardDuty malware iniciada usando ferramentas de linha de AWS comando executando o seguinte AWS CLI comando. Use seu próprio *`ID de detector`* válido.

  > **Note**
  >
  > O código de exemplo a seguir permite a verificação GuardDuty de malware iniciada. Para desabilitá-la, substitua `true` por `false`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
 aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features [{"Name" : "EBS_MALWARE_PROTECTION", "Status" : "ENABLED"}]'
```

Configurando a verificação GuardDuty de malware iniciada em ambientes com várias contas

Em um ambiente com várias contas, somente contas de GuardDuty administrador podem configurar a verificação de GuardDuty malware iniciada. GuardDuty contas de administrador podem ativar ou desativar o uso da verificação de GuardDuty malware iniciada em suas contas de membros. Depois

que a conta do administrador configurar a verificação de GuardDuty malware iniciada para uma conta de membro, a conta de membro seguirá as configurações da conta de administrador e não poderá modificá-las por meio do console. GuardDuty contas de administrador que gerenciam suas contas de membros com AWS Organizations suporte podem optar por ativar automaticamente a verificação de GuardDuty malware iniciada em todas as contas novas e existentes na organização. Para ter mais informações, consulte Gerenciando GuardDuty contas com AWS Organizations.

Estabelecendo acesso confiável para permitir a GuardDuty verificação de malware iniciada

Se a conta de administrador GuardDuty delegado não for igual à conta de gerenciamento em sua organização, a conta de gerenciamento deverá habilitar a verificação de GuardDuty malware iniciada em sua organização. Dessa forma, a conta de administrador delegado pode criar contas de Permissões de função vinculada ao serviço para Proteção contra malware membros que são gerenciadas por meio AWS Organizations de.

> **Note**
>
> Antes de designar uma conta de GuardDuty administrador delegado, consulte. Considerações e recomendações

Escolha seu método de acesso preferido para permitir que a conta de GuardDuty administrador delegado habilite a verificação de GuardDuty malware iniciada para contas de membros na organização.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Para fazer login, use a conta de gerenciamento AWS Organizations da sua organização.

2. a. Se você não designou uma conta de GuardDuty administrador delegado, então:

      Na página Configurações, em Conta de GuardDuty administrador delegado, insira os 12 dígitos **`account ID`** que você deseja designar para administrar a GuardDuty política em sua organização. Escolha Delegar.

   b. i. Se você já designou uma conta de GuardDuty administrador delegado diferente da conta de gerenciamento, então:

Na página Configurações, em Administrador delegado, ative a configuração Permissões. Essa ação permitirá que a conta do GuardDuty administrador delegado anexe permissões relevantes às contas dos membros e habilite a verificação de GuardDuty malware iniciada nessas contas dos membros.

ii. Se você já designou uma conta de GuardDuty administrador delegado que é igual à conta de gerenciamento, você pode ativar diretamente a verificação de GuardDuty malware iniciada para as contas dos membros. Para ter mais informações, consulte Verificação de GuardDuty malware iniciada automaticamente para todas as contas dos membros.

> **Tip**
>
> Se a conta do GuardDuty administrador delegado for diferente da sua conta de gerenciamento, você deverá fornecer permissões à conta do GuardDuty administrador delegado para permitir a ativação da verificação de GuardDuty malware iniciada nas contas dos membros.

3. Se você quiser permitir que a conta de GuardDuty administrador delegado habilite a verificação de GuardDuty malware iniciada para contas de membros em outras regiões, altere a sua Região da AWS e repita as etapas acima.

API/CLI

1. Usando as credenciais da conta de gerenciamento, execute o seguinte comando:

```
aws organizations enable-aws-service-access --service-principal malware-
protection.guardduty.amazonaws.com
```

2. (Opcional) para ativar a verificação de GuardDuty malware iniciada para a conta de gerenciamento que não é uma conta de administrador delegado, a conta de gerenciamento primeiro criará a verificação Permissões de função vinculada ao serviço para Proteção contra malware explícita em sua conta e, em seguida, ativará a verificação de GuardDuty malware iniciada a partir da conta de administrador delegado, semelhante a qualquer outra conta de membro.

```
aws iam create-service-linked-role --aws-service-name malware-
protection.guardduty.amazonaws.com
```

3. Você designou a conta de GuardDuty administrador delegado na conta atualmente selecionada Região da AWS. Se você designou uma conta como conta de GuardDuty administrador delegado em uma região, essa conta deverá ser sua conta de GuardDuty administrador delegado em todas as outras regiões. Repita a etapa acima para todas as outras regiões.

Configurando a verificação de GuardDuty malware iniciada para uma conta de administrador delegado GuardDuty

Escolha seu método de acesso preferido para ativar ou desativar a verificação GuardDuty de malware iniciada para uma conta de GuardDuty administrador delegado.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de gerenciamento.
2. No painel de navegação, escolha Proteção contra malware.
3. Na página Proteção contra malware, escolha Editar ao lado da verificação GuardDuty de malware iniciada.
4. Execute um destes procedimentos:

   Como usar a opção Habilitar para todas as contas

   - Escolha Habilitar para todas as contas. Isso habilitará o plano de proteção para todas as GuardDuty contas ativas em sua AWS organização, incluindo as novas contas que ingressam na organização.
   - Escolha Salvar.

   Como usar a opção Configurar contas manualmente

   - Para ativar o plano de proteção somente para a conta de GuardDuty administrador delegado, escolha Configurar contas manualmente.
   - Escolha Habilitar na seção Conta de GuardDuty administrador delegado (esta conta).

- Escolha Salvar.

API/CLI

Execute a operação da API updateDetector usando seu próprio ID de detector regional e transmitindo o `name` do objeto `features` como `EBS_MALWARE_PROTECTION` e `status` como `ENABLED` ou `DISABLED`.

Você pode ativar ou desativar a verificação GuardDuty de malware iniciada executando o AWS CLI comando a seguir. Certifique-se de usar o *`ID de detector`* válido da conta de GuardDuty administrador delegado.

> **Note**
>
> O código de exemplo a seguir permite a verificação GuardDuty de malware iniciada. Para desabilitá-la, substitua `ENABLED` por `DISABLED`.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 /
              --account-ids 555555555555 /
              --features '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
```

Verificação de GuardDuty malware iniciada automaticamente para todas as contas dos membros

Escolha seu método de acesso preferido para ativar o recurso GuardDuty de verificação de malware iniciado para todas as contas dos membros. Isso inclui contas-membro existentes e as novas contas que ingressam na organização.

Console

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

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. Execute um destes procedimentos:

Como usar a página Proteção contra malware

1. No painel de navegação, escolha Proteção contra malware.
2. Na página Proteção contra malware, escolha Editar na seção de verificação GuardDuty de malware iniciada.
3. Escolha Habilitar para todas as contas. Essa ação ativa automaticamente a verificação GuardDuty de malware iniciada para contas existentes e novas na organização.
4. Escolha Salvar.

> **Note**
>
> Pode levar até 24 horas para atualizar a configuração das contas-membro.

Como usar a página Contas

1. No painel de navegação, escolha Accounts (Contas).
2. Na página Contas, escolha Habilitar automaticamente as preferências antes de Adicionar contas por convite.
3. Na janela Gerenciar preferências de ativação automática, escolha Ativar para todas as contas na verificação de GuardDutymalware iniciada.
4. Na página Proteção contra malware, escolha Editar na seção de verificação GuardDuty de malware iniciada.
5. Escolha Habilitar para todas as contas. Essa ação ativa automaticamente a verificação GuardDuty de malware iniciada para contas existentes e novas na organização.
6. Escolha Salvar.

> **Note**
>
> Pode levar até 24 horas para atualizar a configuração das contas-membro.

Como usar a página Contas

1. No painel de navegação, escolha Accounts (Contas).

2. Na página Contas, escolha Habilitar automaticamente as preferências antes de Adicionar contas por convite.
3. Na janela Gerenciar preferências de ativação automática, escolha Ativar para todas as contas na verificação de GuardDutymalware iniciada.
4. Escolha Salvar.

Se você não conseguir usar a opção Habilitar para todas as contas, consulte Ative ou desative seletivamente a verificação GuardDuty de malware iniciada para contas de membros.

API/CLI

- *Para ativar ou desativar seletivamente a verificação de GuardDuty malware iniciada em suas contas de membros, invoque a operação da updateMemberDetectorsAPI usando seu próprio ID de detector.*
- O exemplo a seguir mostra como você pode ativar a verificação GuardDuty de malware iniciada para uma única conta de membro. Para desabilitar uma conta de membro, substitua `ENABLED` por `DISABLED`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"Name": "EBS_MALWARE_PROTECTION", "Status": "ENABLED"}]'
  ```

  Você também pode passar uma lista de IDs de contas separadas por um espaço.
- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Ativar a verificação GuardDuty de malware iniciada para todas as contas de membros ativas existentes

Escolha seu método de acesso preferido para ativar a verificação de GuardDuty malware iniciada para todas as contas de membros ativos existentes na organização.

Para configurar a verificação GuardDuty de malware iniciada para todas as contas de membros ativas existentes

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

   Faça login usando as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, escolha Proteção contra malware.
3. Na Proteção contra malware, você pode ver o status atual da configuração de verificação de GuardDuty malware iniciada. Na seção Contas-membro ativas, escolha Ações.
4. No menu suspenso Ações, escolha Habilitar para todas as contas-membro ativas existentes.
5. Escolha Salvar.

Verificação de GuardDuty malware iniciada automaticamente para contas de novos membros

As contas de membros recém-adicionadas devem ser ativadas GuardDuty antes de selecionar a configuração da verificação de GuardDuty malware iniciada. As contas dos membros gerenciadas por convite podem configurar manualmente a verificação de GuardDuty malware iniciada por suas contas. Para ter mais informações, consulte Step 3 - Accept an invitation.

Escolha seu método de acesso preferido para ativar a verificação de GuardDuty malware iniciada para novas contas que ingressam na sua organização.

Console

A conta de GuardDuty administrador delegado pode ativar a verificação de GuardDuty malware iniciada para contas de novos membros em uma organização, usando a página Proteção contra malware ou Contas.

Para ativar automaticamente a verificação GuardDuty de malware iniciada para contas de novos membros

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. Execute um destes procedimentos:
   - Como usar a página Proteção contra malware:

     1. No painel de navegação, escolha Proteção contra malware.

2. Na página Proteção contra malware, escolha Editar na verificação GuardDuty de malware iniciada.
3. Escolha Configurar contas manualmente.
4. Selecione Habilitar automaticamente para novas contas-membro. Essa etapa garante que, sempre que uma nova conta ingressar em sua organização, a verificação de GuardDuty malware iniciada seja ativada automaticamente para sua conta. Somente a conta do GuardDuty administrador delegado da organização pode modificar essa configuração.
5. Selecione Salvar.

- Como usar a página Contas:

1. No painel de navegação, escolha Accounts (Contas).
2. Na página Contas, escolha Habilitar automaticamente as preferências.
3. Na janela Gerenciar preferências de ativação automática, selecione Habilitar para novas contas em Análise de GuardDutymalware iniciada.
4. Selecione Salvar.

API/CLI

- Para ativar ou desativar a verificação de GuardDuty malware iniciada para novas contas de membros, invoque a operação da UpdateOrganizationConfigurationAPI usando seu próprio ID de *`detector`*.
- O exemplo a seguir mostra como você pode ativar a verificação GuardDuty de malware iniciada para uma única conta de membro. Para desabilitá-lo, consulte Ative ou desative seletivamente a verificação GuardDuty de malware iniciada para contas de membros. Se não quiser habilitá-lo para todas as novas contas que ingressarem na organização, defina `AutoEnable` como `NONE`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --AutoEnable --features '[{"Name":
 "EBS_MALWARE_PROTECTION", "AutoEnable": NEW}]'
```

  Você também pode passar uma lista de IDs de contas separadas por um espaço.

- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Ative ou desative seletivamente a verificação GuardDuty de malware iniciada para contas de membros

Escolha seu método de acesso preferido para configurar seletivamente a verificação de GuardDuty malware iniciada para contas de membros.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Accounts (Contas).
3. Na página Contas, revise a coluna GuardDutyde verificação de malware iniciada para ver o status da sua conta de membro.
4. Selecione a conta para a qual você deseja configurar GuardDuty - escaneamento de malware iniciado. Você pode selecionar várias contas ao mesmo tempo.
5. No menu Editar planos de proteção, escolha a opção apropriada para a verificação GuardDuty de malware iniciada.

API/CLI

Para ativar ou desativar seletivamente a verificação de GuardDuty malware iniciada em suas contas de membros, invoque a operação da `updateMemberDetectors`API usando seu próprio ID de detector.

O exemplo a seguir mostra como você pode ativar a verificação GuardDuty de malware iniciada para uma única conta de membro. Para desabilitá-la, substitua `ENABLED` por `DISABLED`.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "EBS_MALWARE_PROTECTION",
 "Status": "ENABLED"}]'
```

> **Note**
>
> Você também pode passar uma lista de IDs de contas separadas por um espaço.

Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Para ativar ou desativar seletivamente a verificação de GuardDuty malware iniciada em suas contas de membros, execute a operação da updateMemberDetectorsAPI usando seu próprio ID de *`detector`*. O exemplo a seguir mostra como você pode ativar a verificação GuardDuty de malware iniciada para uma única conta de membro. Para desabilitá-la, substitua `true` por `false`.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 123456789012 --data-sources '{"MalwareProtection":
{"ScanEc2InstanceWithFindings":{"EbsVolumes":true}}}'
```

> **Note**
>
> Você também pode passar uma lista de IDs de contas separadas por um espaço.

Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Ative a verificação GuardDuty de malware iniciada para contas existentes na organização gerenciadas por meio de convite

A função vinculada ao serviço de Proteção contra GuardDuty Malware (SLR) deve ser criada nas contas dos membros. A conta do administrador não pode ativar o recurso GuardDuty de verificação de malware iniciado em contas de membros que não são gerenciadas pelo AWS Organizations.

Atualmente, você pode executar as etapas a seguir por meio do GuardDuty console em https://console.aws.amazon.com/guardduty/ para ativar a verificação de GuardDuty malware iniciada nas contas de membros existentes.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Faça login usando as credenciais da sua conta de administrador.
2. No painel de navegação, escolha Accounts (Contas).
3. Selecione a conta de membro para a qual você deseja ativar a verificação GuardDuty de malware iniciada. Você pode selecionar várias contas ao mesmo tempo.
4. Escolha Ações.
5. Selecione Desassociar membro.
6. Na sua conta-membro, escolha Proteção contra malware em Planos de proteção no painel de navegação.
7. Escolha Ativar GuardDuty escaneamento de malware iniciado. GuardDuty criará uma SLR para a conta do membro. Para obter mais informações sobre a SLR, consulte Permissões de função vinculada ao serviço para Proteção contra malware.
8. Na sua conta de administrador, escolha Contas no painel de navegação.
9. Escolha a conta-membro que precisa ser adicionada novamente à organização.
10. Escolha Ações e selecione Adicionar membro.

API/CLI

1. Use a conta de administrador para executar a DisassociateMembersAPI nas contas de membros que desejam ativar a verificação GuardDuty de malware iniciada.
2. Use sua conta de membro para invocar e ativar UpdateDetectora verificação GuardDuty de malware iniciada.

   Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

   ```
   aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0
    --data-sources '{"MalwareProtection":{"ScanEc2InstanceWithFindings":
   {"EbsVolumes":true}}}'
   ```

3. Use a conta de administrador para executar a CreateMembersAPI e adicionar o membro de volta à organização.

Descobertas que invocam uma verificação GuardDuty de malware iniciada

Uma verificação GuardDuty de malware iniciada é invocada quando GuardDuty detecta um comportamento suspeito indicativo de malware na instância do Amazon EC2 ou nas cargas de trabalho do contêiner.

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS
- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce (Somente de saída)
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS

- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS
- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/RDPBruteForce (Somente de saída)
- UnauthorizedAccess:EC2/SSHBruteForce (Somente de saída)
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay
- Backdoor:Runtime/C&CActivity.B
- Backdoor:Runtime/C&CActivity.B!DNS
- CryptoCurrency:Runtime/BitcoinTool.B
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- Execution:Runtime/NewBinaryExecuted
- Execution:Runtime/NewLibraryLoaded
- Execution:Runtime/ReverseShell
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/CryptoMinerExecuted
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DropPoint
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS

- Trojan:Runtime/PhishingDomainRequest!DNS
- UnauthorizedAccess:Runtime/MetadataDNSRebind

Verificação de malware sob demanda

O verificação de malware sob demanda ajuda você a detectar a presença de malware em volumes do Amazon Elastic Block Store (Amazon EBS) anexados a instâncias do Amazon EC2. Sem a necessidade de configuração, você pode iniciar uma verificação de malware sob demanda fornecendo o nome do recurso da Amazon (ARN) da instância do Amazon EC2 que você deseja verificar. Você pode iniciar uma verificação de malware sob demanda por meio do GuardDuty console ou da API. Antes de iniciar uma verificação de malware sob demanda, você pode definir sua configuração de Retenção de snapshots preferida. Os cenários a seguir podem ajudá-lo a identificar quando usar o tipo de escaneamento de malware sob demanda com GuardDuty:

- Você deseja detectar a presença de malware em suas instâncias do Amazon EC2 sem ativar a verificação de malware GuardDuty iniciada.
- Você ativou a verificação GuardDuty de malware iniciada e uma verificação foi invocada automaticamente. Depois de seguir a correção recomendada para o tipo de descoberta de Proteção contra malware gerado, se você quiser iniciar uma verificação no mesmo recurso, poderá iniciar uma verificação de malware sob demanda após 1 hora do horário de início da verificação anterior.

  O verificação de malware sob demanda não exige que tenham passado 24 horas desde o momento em que o verificação de malware anterior foi iniciado. Deveria ter passado uma hora antes de iniciar uma verificação de malware sob demanda no mesmo recurso. Para evitar a duplicação de uma verificação de malware na mesma instância do EC2, consulte Digitaliza novamente a mesma instância do Amazon EC2.

> **Note**
>
> A verificação de malware sob demanda não está incluída no período de teste gratuito de 30 dias com. GuardDuty O custo de uso se aplica ao volume total do Amazon EBS verificado para cada verificação de malware. Para obter mais informações, consulte os GuardDuty preços da Amazon. Para obter informações sobre os custos de criação dos snapshots de volumes do Amazon EBS e sua retenção, consulte Definição de preços do Amazon EBS.

Como funciona a verificação de malware sob demanda

Com a verificação de malware sob demanda, é possível iniciar uma solicitação de verificação de malware para sua instância do Amazon EC2, mesmo quando ela estiver em uso no momento. Depois de iniciar uma verificação de malware sob demanda, GuardDuty cria instantâneos dos volumes do Amazon EBS anexados à instância do Amazon EC2 cujo Amazon Resource Name (ARN) foi fornecido para a verificação. Em seguida, GuardDuty compartilha esses instantâneos com o. GuardDuty conta de serviço GuardDuty cria volumes de réplica criptografados do EBS a partir desses snapshots na conta de serviço. GuardDuty Para obter mais informações sobre como os volumes do Amazon EBS são verificados, consulte Volume do Elastic Block Storage (EBS).

> **Note**
>
> GuardDuty cria os instantâneos dos dados que já foram gravados nos volumes do Amazon EBS no momento em que você inicia uma verificação de malware sob demanda. point-in-time

Se um malware for encontrado e você tiver habilitado a configuração de retenção de snapshots, os snapshots do seu volume do EBS serão automaticamente retidos na sua Conta da AWS. A verificação de malware sob demanda gera os Tipos de descoberta de Malware Protection. Se o malware não for encontrado, independentemente da configuração de retenção de snapshots, os snapshots dos seus volumes do EBS serão excluídos.

Por padrão, os snapshots dos seus volumes do EBS são criados com uma tag `GuardDutyScanId`. Não remova essa tag, pois isso GuardDuty impedirá o acesso aos instantâneos. Ambos os tipos de varredura na Proteção contra malware não examinam as instâncias do Amazon EC2 ou os volumes do Amazon EBS que têm a tag `GuardDutyExcluded` definida como `true`. Se a Proteção contra malware fizer uma verificação em tal recurso, um ID de verificação será gerado, mas a verificação será ignorada com o motivo `EXCLUDED_BY_SCAN_SETTINGS`. Para ter mais informações, consulte Razões para ignorar o recurso durante a verificação de malware.

AWS Organizations política de controle de serviços — Acesso negado

Usando as políticas de controle de serviços (SCPs) em AWS Organizations, a conta do GuardDuty administrador delegado pode restringir permissões e negar ações, como iniciar uma verificação de malware sob demanda para a instância do Amazon EC2 de propriedade de suas contas.

Como conta GuardDuty membro, ao iniciar uma verificação de malware sob demanda para suas instâncias do Amazon EC2, você pode receber uma mensagem de erro. Você pode se conectar à

conta de gerenciamento para entender por que um SCP foi configurado para sua conta de membro. Para obter mais informações, consulte Efeitos do SCP sobre as permissões.

Conceitos básicos sobe a verificação de malware sob demanda

Como conta de GuardDuty administrador, você pode iniciar uma verificação de malware sob demanda em nome de suas contas de membros ativas que tenham os seguintes pré-requisitos configurados em suas contas. Contas autônomas e contas de membros ativos também GuardDuty podem iniciar uma verificação de malware sob demanda para suas próprias instâncias do Amazon EC2.

Pré-requisitos

- GuardDuty deve estar habilitado no Regiões da AWS local em que você deseja iniciar a verificação de malware sob demanda.
- Verifique se a AWS política gerenciada: AmazonGuardDutyFullAccess está anexada ao usuário do IAM ou ao perfil do IAM. Você precisará da chave de acesso e da chave secreta associadas ao usuário do IAM ou ao perfil do IAM.
- Como conta de GuardDuty administrador delegado, você tem a opção de iniciar uma verificação de malware sob demanda em nome de uma conta de membro ativa.
- Se você for uma conta-membro que não tem as Permissões de função vinculada ao serviço para Proteção contra malware, iniciar uma verificação de malware sob demanda para uma instância do Amazon EC2 que pertence à sua conta criará automaticamente a SLR para Proteção contra malware.

> **Important**
>
> Certifique-se de que ninguém exclua as permissões SLR para proteção contra malware quando a verificação de malware, GuardDuty iniciada ou sob demanda, ainda estiver em andamento. Isso impedirá que a verificação seja concluída com êxito e forneça um resultado definitivo da verificação.

Antes de iniciar uma verificação de malware sob demanda, certifique-se de que nenhuma verificação tenha sido iniciada no mesmo recurso na última 1 hora. Caso contrário, ela será eliminada. Para ter mais informações, consulte Digitalizar novamente o mesmo recurso.

Como iniciar a verificação de malware sob demanda

Selecione seu método de acesso preferido para iniciar uma verificação de malware sob demanda.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. Inicie a verificação usando uma das seguintes opções:

   a. Como usar a página Proteção contra malware:

      i. No painel de navegação, em Planos de proteção, escolha Proteção contra malware.

      ii. Na página Proteção contra malware, forneça o ARN da instância do Amazon EC2[1] para o qual você deseja iniciar a verificação.

   b. Como usar a página Verificações de malware:

      i. No painel de navegação, escolha Verificações de malware.

      ii. Escolha Iniciar verificação sob demanda e forneça o ARN da instância do Amazon EC2[1] para o qual você deseja iniciar o verificação.

      iii. Se for uma nova verificação, selecione um ID de instância do Amazon EC2 na página Verificações de malware.

      Expanda a lista suspensa Iniciar verificação sob demanda e escolha Verificar novamente a instância selecionada.

3. Depois de iniciar com êxito uma verificação usando qualquer um dos métodos, um ID de verificação é gerado. Você pode usar esse ID de verificação para acompanhar o andamento da verificação. Para ter mais informações, consulte Monitoramento de status e resultados de verificação de malware.

API/CLI

Invoke StartMalwareScanthat aceita a [instância] 1 `resourceArn` do Amazon EC2 para a qual você deseja iniciar uma verificação de malware sob demanda.

```
aws guardduty start-malware-scan --resource-arn "arn:aws:ec2:us-
east-1:555555555555:instance/i-b188560f"
```

Depois de iniciar uma verificação com sucesso, `StartMalwareScan` retorna um `scanId`. O Invoke DescribeMalwareScansmonitora o progresso da verificação iniciada.

[1]Para obter informações sobre o formato do ARN da sua instância do Amazon EC2, consulte Nomes de recurso da Amazon (ARN). Para instâncias do Amazon EC2, você pode usar o seguinte exemplo de formato de ARN substituindo os valores da partição, região, ID da Conta da AWS e ID de instância do Amazon EC2. Para obter informações sobre o tamanho do ID da sua instância, consulte IDs de recursos.

```
arn:aws:ec2:us-east-1:555555555555:instance/i-b188560f
```

Digitaliza novamente a mesma instância do Amazon EC2

Independentemente de uma verificação ser GuardDuty iniciada ou sob demanda, você pode iniciar uma nova verificação de malware sob demanda na mesma instância do EC2 após 1 hora a partir da hora de início da verificação de malware anterior. Se a nova verificação de malware for iniciada dentro de 1 hora após o início da verificação de malware anterior, sua solicitação resultará no seguinte erro e nenhuma ID de verificação será gerada para essa solicitação.

```
A scan was initiated on this resource recently. You can request a scan on the same resource one hour after the previous scan start time.
```

Para obter informações sobre como iniciar uma nova verificação no mesmo recurso, consulte Como iniciar a verificação de malware sob demanda.

Para acompanhar o status das verificações de malware, consulte Monitoramento de status de escaneamento e resultados na Proteção GuardDuty contra Malware.

Monitoramento de status de escaneamento e resultados na Proteção GuardDuty contra Malware

Você pode monitorar o status de cada escaneamento do GuardDuty Malware Protection. Os valores possíveis para Status da verificação são `Completed`, `Running`, `Skipped` e `Failed`.

Depois que a verificação for concluída, o Resultado da verificação será preenchido para verificações que têm o Status de `Completed`. Os valores possíveis para o Resultado da verificação são `Clean` e `Infected`. Usando o Tipo de verificação, você pode identificar se a verificação de malware foi `GuardDuty initiated` ou `On demand`.

Os resultados de verificação de cada verificação de malware têm um período de retenção de 90 dias. Escolha seu método de acesso preferido para rastrear o status da verificação de malware.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Verificações de malware.
3. Você pode filtrar as verificações de malware pelas seguintes Propriedades disponíveis nos critérios de filtro.

   - ID de verificação
   - ID da conta
   - ARN da instância do EC2
   - Tipo de verificação
   - Status da verificação

   Para obter informações sobre propriedades usadas para critérios de filtro, consulte Detalhes da descoberta.

API/CLI

- Depois que a verificação de malware tiver um resultado de verificação, você poderá filtrar as verificações de malware com base em `EC2_INSTANCE_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE` `GUARDDUTY_FINDING_ID`, `SCAN_STATUS` e `SCAN_START_TIME`.

  Os critérios do `GUARDDUTY_FINDING_ID` filtro estão disponíveis quando o `SCAN_TYPE` é GuardDuty iniciado. Para obter informações sobre qualquer critério de filtro, consulte Detalhes da descoberta.
- Você pode alterar o exemplo de *`filter-criteria`* no comando abaixo. Atualmente, você pode filtrar com base em uma `CriterionKey` de cada vez. As opções para `CriterionKey` são `EC2_INSTANCE_ARN`, `SCAN_ID`, `ACCOUNT_ID`, `SCAN_TYPE` `GUARDDUTY_FINDING_ID`, `SCAN_STATUS` e `SCAN_START_TIME`.

  Se você usar a mesma `CriterionKey` que a abaixo, certifique-se de substituir o exemplo de `EqualsValue` por seu próprio *`scan-id`* da AWS válido.

Substitua o `detector-id` de exemplo por seu próprio *`detector-id`* válido. Você pode alterar *`max-results`* (até 50) e *`sort-criteria`*. O `AttributeName` é obrigatório e deve ser `scanStartTime`.

```
aws guardduty describe-malware-scans --detector-
id 60b87779336485625 54d637e0e4bb3b2 --max-results 1 --sort-criteria
 '{"AttributeName": "scanStartTime", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"SCAN_ID", "FilterCondition":
{"EqualsValue":"123456789012"}}] }'
```

- A resposta desse comando exibe no máximo um resultado com detalhes sobre o recurso afetado e as descobertas de malware (se `Infected`).

GuardDuty contas de serviço por Região da AWS

Quando um snapshot é criado e compartilhado com uma conta GuardDuty de serviço, um novo evento é criado em seus CloudTrail registros. Esse evento especifica o `snapshotId` e `userId` (conta GuardDuty de serviço correspondente Região da AWS). Para ter mais informações, consulte Atributo na Proteção contra malware.

O exemplo a seguir é um trecho de um CloudTrail evento que mostra o corpo da solicitação: `ModifySnapshotAttribute`

```
"requestParameters": {
        "snapshotId": "snap-1234567890abcdef0",
        "createVolumePermission": {
            "add": {
                "items": [
                    {
                        "userId": "111122223333"
                    }
                ]
            }
        },
        "attributeType": "CREATE_VOLUME_PERMISSION"
    }
```

A tabela a seguir mostra as contas GuardDuty de serviço de cada região. `userId`É a conta GuardDuty de serviço e depende da região selecionada.

Região da AWS	Código da região	GuardDuty ID da conta de serviço (**`userId`**)
Leste dos EUA (Norte da Virgínia)	us-east-1	652050842985
Leste dos EUA (Ohio)	us-east-2	178123968615
Oeste dos EUA (N. da Califórnia)	us-west-1	669213148797
Oeste dos EUA (Oregon)	us-west-2	447226417196
Ásia-Pacífico (Mumbai)	ap-south-1	913179291432
Asia Pacific (Osaka)	ap-northeast-3	089661699081
Ásia-Pacífico (Seul)	ap-northeast-2	039163547507
Ásia-Pacífico (Tóquio)	ap-northeast-1	874749492622
Ásia-Pacífico (Singapura)	ap-southeast-1	247460962669
Ásia-Pacífico (Sydney)	ap-southeast-2	124839743349
Canadá (Central)	ca-central-1	175877067165
Oeste do Canadá (Calgary)	ca-west-1	894794104037
Europa (Frankfurt)	eu-central-1	00:294, 50.712
Europa (Irlanda)	eu-west-1	283769539786
Europa (Londres)	eu-west-2	310125036783
Europa (Paris)	eu-west-3	866607715269
Europa (Estocolmo)	eu-north-1	693780578038
China (Pequim)	cn-north-1	448721096076

Região da AWS	Código da região	GuardDuty ID da conta de serviço (**`userId`**)
China (Ningxia)	cn-northwest-1	480864352451
América do Sul (São Paulo)	sa-east-1	546914126324
Asia Pacific (Hyderabad) (adesão)	ap-south-2	682251015962
Ásia-Pacífico (Melbourne) (adesão)	ap-southeast-4	353488359550
Europa (Espanha) (adesão)	eu-south-2	936182149045
Europa (Zurique) (adesão)	eu-central-2	867642063380
Israel (Tel Aviv) (adesão)	il-central-1	619233833001
Europa (Milão) (adesão)	eu-south-1	977238331021
Ásia-Pacífico (Hong Kong) (adesão)	ap-east-1	249472122084
Oriente Médio (Bahrein) (adesão)	me-south-1	404001805210
África (Cidade do Cabo) (adesão)	af-south-1	957664736811
Ásia-Pacífico (Jacarta) (adesão)	ap-southeast-3	452118225523
Oriente Médio (Emirados Árabes Unidos) (adesão)	me-central-1	828603743433

Cotas de Proteção contra malware

A Proteção contra malware tem a seguinte disponibilidade padrão de vários recursos que o atributo usa.

Escopo	Padrão	Comentários
Extração e análise de dados em arquivo comprimido ou compactado	5	O número máximo de níveis aninhados permitidos em um arquivo compactado.
Número de arquivos em um arquivo compactado	1000	O número máximo de arquivos que podem ser verificados em um arquivo compactado. Essa contagem é a soma do número de arquivos extraídos do arquivo compactado e do número de arquivos extraídos de todos os arquivos compactados aninhados.
Número de ameaças	32	O número máximo de ameaças que você pode ver no painel de descobertas. GuardDuty A Proteção contra Malware pode ter detectado mais nomes de ameaças. Se o número de nomes de ameaças detectados for maior que o valor padrão, você poderá visualizar os detalhes do JSON seleciona ndo o ID de busca abaixo do nome da descoberta no painel de detalhes do GuardDuty console.

Escopo	Padrão	Comentários
Número de arquivos por ameaça detectada	5	O número máximo de arquivos identificados por ameaça detectada. Por exemplo, se GuardDuty detectar 10 arquivos associados a uma única ameaça, a ameaça exibirá no máximo 5 arquivos.
Volumes do EBS por verificação por instância	11	O número máximo de volumes do EBS que GuardDuty podem ser escaneados por instância do EC2. Se houver mais de 11 volumes do EBS que precisam ser verificados, o GuardDuty Malware Protection os classifica em `deviceName` ordem alfabética e seleciona os primeiros 11 volumes do EBS.
Tamanho do volume do EBS	1024 GB	O tamanho máximo do volume do EBS em GB que o GuardDuty Malware Protection pode verificar em cada região.

Escopo	Padrão	Comentários
Tipos de sistemas de arquivos com suporte	GuardDuty A Proteção contra Malware pode verificar os seguintes tipos de sistema de arquivos: • Sistema de arquivos New Technology (NTFS) • Sistema de arquivos X (XFS) • Segundo sistema de arquivos estendido (ext2) • Quarto sistema de arquivos estendido (ext4) • Sistema de arquivos da tabela de alocação de arquivos (FAT) • Sistema de arquivos da tabela de alocação de arquivos virtuais (VFAT)	N/D
Tags de opções de verificação	50	O número máximo de tags de recursos que podem ser adicionadas para personalizar sua configuração de opções de verificação de malware. Para ter mais informações, consulte Opções de verificação com tags definidas pelo usuário.

Escopo	Padrão	Comentários
Período de retenção da descoberta	90	O número máximo de dias que GuardDuty retém uma descoberta. Para obter as informações mais recentes, consulte Cotas para a Amazon GuardDuty.
Período de retenção de verificação de malware	90	O número máximo de dias em que o GuardDuty Malware Protection retém o histórico de um escaneamento. Para obter mais informações sobre como visualizar verificações recentes de malware, consulte Monitoramento de status de escaneamento e resultados na Proteção GuardDuty contra Malware.
Transações por segundo (TPS) para verificação de malware sob demanda	1	O número de solicitações de verificação de malware sob demanda que podem ser iniciadas por segundo em cada região.
Limite de intermitência para verificação de malware sob demanda	1	O número de solicitações simultâneas de verificação de malware sob demanda que podem ser iniciadas por segundo em cada região.

GuardDuty Proteção RDS

A Proteção do RDS na Amazon GuardDuty analisa e traça o perfil da atividade de login do RDS para possíveis ameaças de acesso aos seus bancos de dados Amazon Aurora (Amazon Aurora MySQL Compatible Edition e Aurora PostgreSQL Compatible Edition). Esse recurso permite identificar comportamentos de login potencialmente suspeitos. A Proteção do RDS não requer infraestrutura adicional. Ela foi projetada para não afetar a performance de suas instâncias de banco de dados.

Quando o RDS Protection detecta uma tentativa de login potencialmente suspeita ou anômala que indica uma ameaça ao seu banco de dados, GuardDuty gera uma nova descoberta com detalhes sobre o banco de dados potencialmente comprometido.

Você pode ativar ou desativar o recurso de Proteção RDS para qualquer conta em qualquer Região da AWS lugar em que esse recurso esteja disponível na Amazon GuardDuty, a qualquer momento. Uma GuardDuty conta existente pode ativar a Proteção RDS com um período de teste de 30 dias. Para uma nova GuardDuty conta, a Proteção RDS já está ativada e incluída no período de teste gratuito de 30 dias. Para ter mais informações, consulte Como estimar os custos.

> **Note**
>
> Quando o recurso de Proteção do RDS não está ativado, GuardDuty ele não coleta sua atividade de login do RDS nem detecta comportamentos de login anômalos ou suspeitos.

Para obter informações sobre o Regiões da AWS where ainda GuardDuty não oferece suporte à Proteção RDS, consulteDisponibilidade de recursos específicos da região.

Bancos de dados do Amazon Aurora compatíveis

A tabela a seguir mostra para as versões do banco de dados do Aurora compatíveis.

Mecanismo de bancos de dados Amazon Aurora	Versões compatíveis do mecanismo
Aurora MySQL	• 2.10.2 ou posterior • 3.02.1 ou posterior

Mecanismo de bancos de dados Amazon Aurora	Versões compatíveis do mecanismo
Aurora PostgreSQL	• 10.17 ou posterior • 11.12 ou posterior • 12.7 ou posterior • 13.3 ou posterior • 14.3 ou posterior • 15.2 ou posterior • 16.1 ou posterior

Como a Proteção do RDS usa o monitoramento de atividades de login do RDS

A Proteção do RDS na Amazon GuardDuty ajuda você a proteger os bancos de dados Amazon Aurora (Aurora) compatíveis em sua conta. Depois de ativar o recurso de Proteção do RDS, começa GuardDuty imediatamente a monitorar a atividade de login do RDS nos bancos de dados do Aurora em sua conta. GuardDuty monitora e perfila continuamente a atividade de login do RDS em busca de atividades suspeitas, por exemplo, acesso não autorizado ao banco de dados do Aurora em sua conta, de um agente externo nunca antes visto. Quando você habilita a Proteção do RDS pela primeira vez ou tem uma instância de banco de dados recém-criada, é necessário um período de aprendizado para definir o comportamento normal. Por esse motivo, instâncias de banco de dados recém-habilitadas ou recém-criadas podem não ter uma descoberta de login anômala associada por até duas semanas. Para ter mais informações, consulte Monitoramento da atividade de login do RDS.

Quando o RDS Protection detecta uma ameaça em potencial, como um padrão incomum em uma série de tentativas de login bem-sucedidas, malsucedidas ou incompletas, GuardDuty gera uma nova descoberta com detalhes sobre a instância de banco de dados potencialmente comprometida. Para ter mais informações, consulte Tipos de descoberta do RDS Protection. Se você desabilitar a Proteção do RDS, interromperá GuardDuty imediatamente o monitoramento da atividade de login do RDS e não conseguirá detectar nenhuma ameaça potencial às instâncias de banco de dados suportadas.

> **Note**
>
> GuardDuty não gerencia sua atividade de login Bancos de dados compatíveis ou do RDS, nem disponibiliza a atividade de login do RDS para você.

Configuração da Proteção do RDS para uma conta autônoma

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Proteção do RDS.
3. A página Proteção do RDS mostra o status atual da sua conta. Você pode habilitar ou desabilitar o recurso a qualquer momento selecionando Habilitar ou Desabilitar. Confirme a seleção.

API/CLI

Execute a operação da API updateDetector usando seu próprio ID de detector regional e transmitindo o `name` do objeto `features` como `RDS_LOGIN_EVENTS` e `status` como `ENABLED` ou `DISABLED`.

Você também pode ativar ou desativar a Proteção do RDS executando o AWS CLI comando a seguir. Use seu próprio *`ID de detector`* válido.

> **Note**
>
> O código de exemplo a seguir habilita a Proteção do RDS. Para desabilitá-la, substitua `ENABLED` por `DISABLED`.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "RDS_LOGIN_EVENTS", "Status" : "ENABLED"}]'
```

Configuração da proteção do RDS em ambientes de várias contas

Em um ambiente de várias contas, somente a conta de GuardDuty administrador delegado tem a opção de ativar ou desativar o recurso de Proteção RDS para as contas membros em sua organização. As contas GuardDuty dos membros não podem modificar essa configuração em suas contas. A conta de GuardDuty administrador delegado gerencia suas contas de membros usando AWS Organizations. Essa conta de GuardDuty administrador delegado pode optar por ativar automaticamente o monitoramento da atividade de login do RDS para todas as novas contas à medida que elas ingressam na organização. Para obter mais informações sobre ambientes com várias contas, consulte Gerenciamento de várias contas na Amazon. GuardDuty

Configurando a Proteção RDS para uma conta de administrador delegado GuardDuty

Escolha seu método de acesso preferido para configurar o RDS Login Activity Monitoring para a conta de GuardDuty administrador delegado.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de gerenciamento.
2. No painel de navegação, escolha Proteção do RDS.
3. Na página Proteção do RDS, escolha Editar.
4. Execute um destes procedimentos:

   Como usar a opção Habilitar para todas as contas

   - Escolha Habilitar para todas as contas. Isso habilitará o plano de proteção para todas as GuardDuty contas ativas em sua AWS organização, incluindo as novas contas que ingressam na organização.
   - Escolha Salvar.

   Como usar a opção Configurar contas manualmente

   - Para ativar o plano de proteção somente para a conta de GuardDuty administrador delegado, escolha Configurar contas manualmente.
   - Escolha Habilitar na seção Conta de GuardDuty administrador delegado (esta conta).
   - Escolha Salvar.

API/CLI

Execute a operação da API updateDetector usando seu próprio ID de detector regional e transmitindo o `name` do objeto `features` como `RDS_LOGIN_EVENTS` e `status` como `ENABLED` ou `DISABLED`.

Você pode ativar ou desativar a Proteção do RDS executando o AWS CLI comando a seguir. Certifique-se de usar o *`ID de detector`* válido da conta de GuardDuty administrador delegado.

> **Note**
>
> O código de exemplo a seguir habilita a Proteção do RDS. Para desabilitá-la, substitua `ENABLED` por `DISABLED`.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 555555555555 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

Habilitar automaticamente a Proteção do RDS para todas as contas-membro

Escolha seu método de acesso preferido para habilitar o recurso de Proteção do RDS para todas as contas-membro. Isso inclui contas-membro existentes e as novas contas que ingressam na organização.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.

2. Execute um destes procedimentos:

   Como usar a página Proteção do RDS

   1. No painel de navegação, escolha Proteção do RDS.

2. Escolha Habilitar para todas as contas. Essa ação habilita automaticamente a Proteção do RDS para contas novas e existentes na organização.
3. Escolha Salvar.

> **Note**
>
> Pode levar até 24 horas para atualizar a configuração das contas-membro.

Como usar a página Contas

1. No painel de navegação, escolha Accounts (Contas).
2. Na página Contas, escolha Habilitar automaticamente as preferências antes de Adicionar contas por convite.
3. Na janela Gerenciar preferências de habilitação automática, escolha Habilitar para todas as contas em Monitoramento de atividades de login do RDS.
4. Escolha Salvar.

Se você não conseguir usar a opção Habilitar para todas as contas, consulte Habilitar ou desabilitar seletivamente a Proteção do RDS para contas-membro.

API/CLI

- Para habilitar ou desabilitar seletivamente a Proteção do RDS para suas contas-membro, invoque a operação da API updateMemberDetectors usando seu próprio *ID de detector*.
- O exemplo a seguir mostra como você pode habilitar a Proteção do RDS para uma única conta-membro. Para desabilitá-la, substitua `ENABLED` por `DISABLED`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
```

> **Note**
>
> Você também pode passar uma lista de IDs de contas separadas por um espaço.

- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Habilitar a Proteção do RDS para todas as contas-membro ativas existentes

Escolha seu método de acesso preferido para habilitar a Proteção do RDS para todas as contas-membro ativas existentes em sua organização.

Console

Para configurar a Proteção do RDS para todas as contas-membro ativas existentes

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

   Faça login usando as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, escolha Proteção do RDS.
3. Na página Proteção do RDS, você pode ver o status atual da configuração. Na seção Contas-membro ativas, escolha Ações.
4. No menu suspenso Ações, escolha Habilitar para todas as contas-membro ativas existentes.
5. Selecione a opção Confirmar.

API/CLI

- Para habilitar ou desabilitar seletivamente a Proteção do RDS para suas contas-membro, invoque a operação da API updateMemberDetectors usando seu próprio *`ID de detector`*.
- O exemplo a seguir mostra como você pode habilitar a Proteção do RDS para uma única conta-membro. Para desabilitá-la, substitua `ENABLED` por `DISABLED`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "RDS_LOGIN_EVENTS", "status": "ENABLED"}]'
```

> **Note**
>
> Você também pode passar uma lista de IDs de contas separadas por um espaço.

- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Habilitar automaticamente a Proteção do RDS para novas contas-membro

Escolha seu método de acesso preferido para habilitar a atividade de login do RDS para novas contas que ingressarem na sua organização.

Console

A conta de GuardDuty administrador delegado pode habilitar novas contas de membros em uma organização por meio do console, usando a página Proteção do RDS ou Contas.

Para habilitar automaticamente a Proteção do RDS para novas contas-membro

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.
2. Execute um destes procedimentos:
   - Como usar a página Proteção do RDS:
     1. No painel de navegação, escolha Proteção do RDS.
     2. Na página Proteção do RDS, escolha Editar.
     3. Escolha Configurar contas manualmente.
     4. Selecione Habilitar automaticamente para novas contas-membro. Essa etapa garante que, sempre que uma nova conta ingressar na sua organização, a Proteção do RDS seja habilitada automaticamente para a conta dessa pessoa. Somente a conta do GuardDuty administrador delegado da organização pode modificar essa configuração.

5. Selecione Salvar.

- Como usar a página Contas:

1. No painel de navegação, escolha Accounts (Contas).
2. Na página Contas, escolha Habilitar automaticamente as preferências.
3. Na janela Gerenciar preferências de habilitação automática, selecione Habilitar para novas contas em Monitoramento de atividades de login do RDS.
4. Escolha Salvar.

API/CLI

- Para habilitar ou desabilitar seletivamente a Proteção do RDS para suas contas-membro, invoque a operação da API UpdateOrganizationConfiguration usando seu próprio *`ID de detector`*.
- O exemplo a seguir mostra como você pode habilitar a Proteção do RDS para uma única conta-membro. Para desabilitá-lo, consulte Habilitar ou desabilitar seletivamente a Proteção do RDS para contas-membro. Se não quiser habilitá-lo para todas as novas contas que ingressarem na organização, defina `autoEnable` como `NONE`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "RDS_LOGIN_EVENTS", "AutoEnable": "NEW"}]'
```

> **Note**
>
> Você também pode passar uma lista de IDs de contas separadas por um espaço.

- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Habilitar ou desabilitar seletivamente a Proteção do RDS para contas-membro

Escolha seu método de acesso preferido para habilitar ou desabilitar seletivamente o monitoramento da atividade de login do RDS para contas-membro.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.

2. No painel de navegação, escolha Accounts (Contas).

   Na página Contas, revise a coluna Atividade de login do RDS para ver o status da sua conta-membro.

3. Para habilitar ou desabilitar seletivamente a atividade de login do RDS

   Selecione a conta para a qual deseja configurar a Proteção do RDS. Você pode selecionar várias contas ao mesmo tempo. No menu suspenso Editar planos de proteção, escolha Atividade de login do RDS e escolha a opção apropriada.

API/CLI

Para habilitar ou desabilitar seletivamente a Proteção do RDS para suas contas-membro, invoque a operação da API updateMemberDetectors usando seu próprio *ID de detector*.

O exemplo a seguir mostra como você pode habilitar a Proteção do RDS para uma única conta-membro. Para desabilitá-la, substitua `ENABLED` por `DISABLED`.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

> **Note**
>
> Você também pode passar uma lista de IDs de contas separadas por um espaço.

Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Atributo na Proteção do RDS

Monitoramento da atividade de login do RDS

A atividade de login do RDS captura as tentativas de login bem-sucedidas e malsucedidas feitas nos Bancos de dados do Amazon Aurora compatíveis em seu ambiente da AWS . Para ajudá-lo a proteger seus bancos de dados, o GuardDuty RDS Protection monitora continuamente a atividade de login em busca de tentativas de login potencialmente suspeitas. Por exemplo, um invasor pode tentar acessar por força bruta um banco de dados Amazon Aurora adivinhando a senha do banco de dados.

Quando você ativa o recurso de Proteção do RDS, começa GuardDuty automaticamente a monitorar a atividade de login do RDS para seus bancos de dados diretamente do serviço Aurora. Se houver uma indicação de comportamento anômalo de login, GuardDuty gera uma descoberta com detalhes sobre o banco de dados potencialmente comprometido. Quando você habilita a Proteção do RDS pela primeira vez ou tem uma instância de banco de dados recém-criada, é necessário um período de aprendizado para definir o comportamento normal. Por esse motivo, instâncias de banco de dados recém-habilitadas ou recém-criadas podem não ter uma descoberta de login anômala associada por até duas semanas.

O recurso de proteção do RDS não exige nenhuma configuração adicional; ele não afeta nenhuma das configurações existentes do banco de dados Amazon Aurora. GuardDuty não gerencia seus bancos de dados suportados nem a atividade de login do RDS, nem disponibiliza a atividade de login do RDS para você.

Se você optar por ativar automaticamente o recurso de Proteção RDS para novas contas de membros quando elas ingressarem na sua organização, essa ação será ativada automaticamente GuardDuty para essas novas contas de membros. Para obter mais informações sobre como configurar o monitoramento da atividade de login do RDS como um atributo, consulte GuardDuty Proteção RDS.

GuardDuty Monitoramento de execução

O Runtime Monitoring observa e analisa eventos em nível de sistema operacional, rede e arquivos para ajudá-lo a detectar possíveis ameaças em cargas de AWS trabalho específicas em seu ambiente.

GuardDuty lançou inicialmente o Runtime Monitoring para oferecer suporte somente aos recursos do Amazon Elastic Kubernetes Service (Amazon EKS). No entanto, agora você também pode usar o recurso Runtime Monitoring para fornecer detecção de ameaças para seus recursos do AWS Fargate Amazon Elastic Container Service (Amazon ECS) e do Amazon Elastic Compute Cloud (Amazon EC2).

Neste documento e em outras seções relacionadas ao Runtime Monitoring, GuardDuty usa a terminologia do tipo de recurso para se referir aos recursos do Amazon EKS, do Fargate, do Amazon ECS e do Amazon EC2.

O Runtime Monitoring usa um agente de GuardDuty segurança que adiciona visibilidade ao comportamento do tempo de execução, como acesso a arquivos, execução de processos, argumentos de linha de comando e conexões de rede. Para cada tipo de recurso que você deseja monitorar para possíveis ameaças, você pode gerenciar o agente de segurança para esse tipo de recurso específico de forma automática ou manual (com exceção do Fargate (somente Amazon ECS)). Gerenciar o agente de segurança automaticamente significa que você permite GuardDuty instalar e atualizar o agente de segurança em seu nome. Por outro lado, ao gerenciar manualmente o agente de segurança de seus recursos, você é responsável por instalar e atualizar o agente de segurança, conforme necessário.

Com esse recurso estendido, GuardDuty pode ajudá-lo a identificar e responder a possíveis ameaças que podem atingir aplicativos e dados em execução em suas cargas de trabalho e instâncias individuais. Por exemplo, uma ameaça pode começar comprometendo um único contêiner que executa um aplicativo web vulnerável. Esse aplicativo da web pode ter permissões de acesso aos contêineres e cargas de trabalho subjacentes. Nesse cenário, credenciais configuradas incorretamente podem levar a um acesso mais amplo à conta e aos dados armazenados nela.

Ao analisar os eventos de tempo de execução dos contêineres e cargas de trabalho individuais, é GuardDuty possível identificar o comprometimento de um contêiner e das AWS credenciais associadas em uma fase inicial e detectar tentativas de escalar privilégios, solicitações de API suspeitas e acesso malicioso aos dados em seu ambiente.

Conteúdo

Como funcionam

Para usar o Runtime Monitoring, você deve habilitar o Runtime Monitoring e, em seguida, gerenciar o agente GuardDuty de segurança. A lista a seguir explica esse processo em duas etapas:

1. Ative o monitoramento de tempo de execução para sua conta para que ela GuardDuty possa aceitar os eventos de tempo de execução que ela recebe de suas instâncias do Amazon EC2, clusters do Amazon ECS e cargas de trabalho do Amazon EKS.
2. Gerencie o GuardDuty agente para os recursos individuais para os quais você deseja monitorar o comportamento do tempo de execução. Com base no tipo de recurso, você pode optar por implantar o agente de GuardDuty segurança manualmente ou permitindo que GuardDuty ele seja gerenciado em seu nome, o que é chamado de configuração automatizada do agente.

   GuardDuty usa funções de identidade de instância que autenticam o agente de segurança para cada tipo de recurso para enviar os eventos de tempo de execução associados ao VPC endpoint.

> **Note**
>
> GuardDuty não gerencia os eventos de tempo de execução de suas instâncias do Amazon EC2, clusters do Amazon ECS ou clusters do Amazon EKS, nem os torna acessíveis para você.

Quando você gerencia o agente de segurança (manualmente ou por meio de GuardDuty) no EKS Runtime Monitoring ou Runtime Monitoring para instâncias EC2, e atualmente GuardDuty está implantado em uma instância Tipos de eventos de runtime coletados do Amazon EC2 e os recebe dessa instância, não GuardDuty cobrará pela análise dos registros de fluxo Conta da AWS de VPC dessa instância do Amazon EC2. Isso ajuda a GuardDuty evitar o dobro do custo de uso na conta.

Os tópicos a seguir explicam como a ativação do Runtime Monitoring e o gerenciamento do agente de GuardDuty segurança funcionam de forma diferente para cada tipo de recurso.

Conteúdo

Como o Runtime Monitoring funciona com instâncias do Amazon EC2

Suas instâncias do Amazon EC2 podem executar vários tipos de aplicativos e cargas de trabalho em seu ambiente. AWS Quando você ativa o Runtime Monitoring e gerencia o agente de GuardDuty segurança, GuardDuty ajuda a detectar ameaças em suas instâncias existentes do Amazon EC2 e em instâncias potencialmente novas. Esse recurso também oferece suporte às instâncias do Amazon EC2 gerenciadas pelo Amazon EC2.

A ativação do monitoramento de tempo de execução GuardDuty prepara o consumo de eventos de tempo de execução dos processos atualmente em execução e de novos processos nas instâncias do Amazon EC2. GuardDuty exige que um agente de segurança envie eventos de tempo de execução da sua instância do EC2 para o. GuardDuty

Para instâncias do Amazon EC2, o agente GuardDuty de segurança opera no nível da instância. Você pode decidir se deseja monitorar todas ou seletivas instâncias do Amazon EC2 em sua conta.

Se você quiser gerenciar instâncias seletivas, o agente de segurança é necessário somente para essas instâncias.

GuardDuty também pode consumir eventos de tempo de execução de novas tarefas e tarefas existentes em execução nas instâncias do Amazon EC2 dentro dos clusters do Amazon ECS.

Para instalar o agente GuardDuty de segurança, o Runtime Monitoring fornece as duas opções a seguir:

- Use a configuração automatizada do agente (recomendado), ou
- Gerencie o agente de segurança manualmente

Use a configuração automatizada do agente por meio de GuardDuty (recomendado)

Use a configuração automatizada do agente que permita GuardDuty instalar o agente de segurança em suas instâncias do Amazon EC2 em seu nome. GuardDuty também gerencia as atualizações do agente de segurança.

Por padrão, GuardDuty instala o agente de segurança em todas as instâncias da sua conta. Se você quiser GuardDuty instalar e gerenciar o agente de segurança somente para instâncias EC2 selecionadas, adicione tags de inclusão ou exclusão às suas instâncias do EC2, conforme necessário.

Às vezes, você pode não querer monitorar eventos de tempo de execução para todas as instâncias do Amazon EC2 que pertencem à sua conta. Para casos em que você quiser monitorar os eventos de tempo de execução de um número limitado de instâncias, adicione uma tag de inclusão como`GuardDutyManaged`: `true` a essas instâncias selecionadas. Começando com a disponibilidade da configuração automatizada do agente para o Amazon EC2, se sua instância do EC2 tiver uma tag de inclusão (`GuardDutyManaged`:`true`), GuardDuty respeitará a tag e gerenciará o agente de segurança para as instâncias selecionadas, mesmo quando você não habilitar explicitamente a configuração automática do agente.

Por outro lado, se houver um número limitado de instâncias do EC2 para as quais você não deseja monitorar eventos de tempo de execução, adicione uma tag de exclusão (`GuardDutyManaged`:`false`) a essas instâncias selecionadas. GuardDuty honrará a etiqueta de exclusão ao não instalar nem gerenciar o agente de segurança desses recursos do EC2.

Impacto

Ao usar a configuração automatizada de agentes em uma Conta da AWS ou em uma organização, você GuardDuty permite realizar as seguintes etapas em seu nome:

- GuardDuty cria uma associação SSM para todas as suas instâncias do Amazon EC2 que são gerenciadas por SSM e aparecem no Fleet Manager no console https://console.aws.amazon.com/systems-manager/.
- Uso de tags de inclusão com a configuração automática do agente desativada — Depois de ativar o Runtime Monitoring, quando você não ativa a configuração automática do agente, mas adiciona a tag de inclusão à sua instância do Amazon EC2, isso significa que você está autorizando GuardDuty o gerenciamento do agente de segurança em seu nome. A associação SSM então instalará o agente de segurança em cada instância que tiver a tag de inclusão (`GuardDutyManaged:true`).
- Se você ativar a configuração automatizada do agente, a associação SSM instalará o agente de segurança em todas as instâncias do EC2 pertencentes à sua conta.
- Uso de tags de exclusão com configuração automática de agentes — Antes de ativar a configuração automática do agente, ao adicionar uma tag de exclusão à sua instância do Amazon EC2, significa que você está GuardDuty permitindo impedir a instalação e o gerenciamento do agente de segurança para essa instância selecionada.

  Agora, quando você ativa a configuração automatizada do agente, a associação SSM instala e gerencia o agente de segurança em todas as instâncias do EC2, exceto aquelas que estão marcadas com a tag de exclusão.
- GuardDuty cria VPC endpoints em todas as VPCs, incluindo VPCs compartilhadas, desde que haja pelo menos uma instância Linux EC2 nessa VPC que não esteja nos estados de instância encerrada ou encerrada. Para obter informações sobre diferentes estados de instância, consulte o ciclo de vida da instância no Guia do usuário do Amazon EC2 para instâncias Linux.

  GuardDuty também suportaUsando VPC compartilhada com agentes de segurança automatizados. Quando todos os pré-requisitos forem considerados, sua organização GuardDuty usará a VPC compartilhada para receber eventos de tempo de execução. Conta da AWS

> **Note**
>
> Não há custo adicional para o uso dos VPC endpoints criados. GuardDuty

Gerencie o agente de segurança manualmente

Há duas maneiras de gerenciar manualmente o agente de segurança do Amazon EC2:

- Use documentos GuardDuty gerenciados AWS Systems Manager para instalar o agente de segurança em suas instâncias do Amazon EC2 que já são gerenciadas por SSM.

  Sempre que você iniciar uma nova instância do Amazon EC2, certifique-se de que ela esteja habilitada para SSM.
- Use scripts do gerenciador de pacotes RPM (RPM) para instalar o agente de segurança em suas instâncias do Amazon EC2, sejam elas gerenciadas por SSM ou não.

Próxima etapa

Para começar a usar a configuração do Runtime Monitoring para monitorar suas instâncias do Amazon EC2, consulte. Pré-requisitos para suporte à instância do Amazon EC2

Como o Runtime Monitoring funciona com o Fargate (somente para Amazon ECS)

Quando você ativa o Runtime Monitoring, GuardDuty fica pronto para consumir os eventos de tempo de execução de uma tarefa. Essas tarefas são executadas nos clusters do Amazon ECS, que por sua vez são executados nas AWS Fargate (Fargate) instâncias. GuardDuty Para receber esses eventos de tempo de execução, você deve usar o agente de segurança dedicado e totalmente gerenciado.

Atualmente, o Runtime Monitoring não oferece suporte às tarefas iniciadas por AWS Batch e. AWS CodePipeline

Atualmente, o Runtime Monitoring oferece suporte ao gerenciamento do agente de segurança para seus clusters do Amazon ECS (AWS Fargate) somente por meio de. GuardDuty Não há suporte para gerenciar o agente de segurança manualmente nos clusters do Amazon ECS.

Você pode GuardDuty permitir o gerenciamento do agente GuardDuty de segurança em seu nome, usando a configuração automatizada do agente para uma AWS conta ou organização. GuardDuty começará a implantar o agente de segurança nas novas tarefas do Fargate que são lançadas em seus clusters do Amazon ECS. A lista a seguir especifica o que esperar quando você ativa o agente GuardDuty de segurança.

Impacto da ativação do agente GuardDuty de segurança

GuardDuty cria um endpoint de nuvem privada virtual (VPC)

Quando você implanta o agente GuardDuty de segurança, GuardDuty cria um VPC endpoint por meio do qual o agente de segurança entrega os eventos de tempo de execução. GuardDuty

GuardDuty adiciona um contêiner de sidecar

Para uma nova tarefa ou serviço do Fargate que começa a ser executado, um GuardDuty contêiner (sidecar) se conecta a cada contêiner dentro da tarefa do Amazon ECS Fargate. O agente GuardDuty de segurança é executado dentro do GuardDuty contêiner anexado. Isso ajuda GuardDuty a coletar os eventos de tempo de execução de cada contêiner em execução nessas tarefas.

Quando você inicia uma tarefa do Fargate, caso o GuardDuty contêiner (sidecar) não possa ser iniciado em um estado íntegro, o Runtime Monitoring foi projetado para não impedir que as tarefas sejam executadas.

Por padrão, uma tarefa do Fargate é imutável. GuardDuty não implantará o sidecar quando uma tarefa já estiver em execução. Se quiser monitorar um contêiner em uma tarefa já em execução, você pode interromper a tarefa e iniciá-la novamente.

Como o Runtime Monitoring funciona com clusters Amazon EKS

O Runtime Monitoring usa um complemento EKS `aws-guardduty-agent`, também chamado de agente GuardDuty de segurança. Depois que o agente de GuardDuty segurança é implantado em seus clusters EKS, GuardDuty é capaz de receber eventos de tempo de execução para esses clusters EKS.

Você pode monitorar os eventos de tempo de execução dos seus clusters do Amazon EKS no nível da conta ou do cluster. Você pode gerenciar o agente GuardDuty de segurança somente para os clusters do Amazon EKS que você deseja monitorar para detecção de ameaças. Você pode gerenciar o agente GuardDuty de segurança manualmente ou permitindo que GuardDuty ele seja gerenciado em seu nome, usando a configuração automatizada do agente.

Quando você usa a abordagem de configuração automática de agentes GuardDuty para permitir o gerenciamento da implantação do agente de segurança em seu nome, ele cria automaticamente um endpoint da Amazon Virtual Private Cloud (Amazon VPC). O agente de segurança entrega os eventos de tempo de execução GuardDuty usando esse endpoint da Amazon VPC.

Atualmente, GuardDuty oferece suporte a clusters do Amazon EKS em execução em instâncias do Amazon EC2. GuardDuty não é compatível com clusters do Amazon EKS em execução no AWS Fargate.

Após a configuração de monitoramento de tempo de execução

Avalie a cobertura da execução

Depois de habilitar o Runtime Monitoring e implantar o agente de GuardDuty segurança, recomendamos que você avalie continuamente [1] o status de cobertura do recurso em que você implantou o agente de segurança. O status da cobertura pode ser saudável ou insalubre. Um status de cobertura íntegra indica que GuardDuty está recebendo os eventos de tempo de execução do recurso correspondente quando há uma atividade no nível do sistema operacional.

Quando o status da cobertura se torna íntegro para o recurso, GuardDuty é capaz de receber os eventos de tempo de execução e analisá-los para detecção de ameaças. Quando GuardDuty detecta uma possível ameaça à segurança nas tarefas ou aplicativos em execução nas cargas de trabalho e instâncias do seu contêiner, GuardDuty gera um ou mais tipos de descoberta do Runtime Monitoring.

[1] Você também pode configurar uma Amazon EventBridge (EventBridge) para receber uma notificação quando o status da cobertura mudar de Insalubre para Saudável ou de outra forma.

Para ter mais informações, consulte Avaliando a cobertura de tempo de execução de seus recursos.

GuardDuty detecta ameaças potenciais

Quando GuardDuty começa a receber os eventos de tempo de execução do seu recurso, ele começa a analisar esses eventos. Quando GuardDuty detecta uma possível ameaça à segurança em qualquer uma de suas instâncias do Amazon EC2, clusters do Amazon ECS ou clusters do Amazon EKS, ela gera uma ou mais. Tipos de descoberta de monitoramento de tempo de execução Você pode acessar os detalhes da descoberta para visualizar os detalhes do recurso afetado.

Como funciona o teste gratuito de 30 dias no Runtime Monitoring

O período de teste gratuito de 30 dias funciona de forma diferente para as novas GuardDuty contas e as contas existentes que já habilitaram o EKS Runtime Monitoring antes de a capacidade de Runtime Monitoring ser estendida às instâncias do Amazon EC2 e AWS Fargate (somente Amazon ECS).

Estou usando o período de GuardDuty teste ou nunca habilitei o EKS Runtime Monitoring

A lista a seguir explica como o período de teste gratuito de 30 dias funciona se você estiver usando o período de teste de GuardDuty 30 dias ou nunca tiver ativado o EKS Runtime Monitoring:

- Quando você ativa GuardDuty pela primeira vez, o Runtime Monitoring e o EKS Runtime Monitoring não serão ativados por padrão.

  Ao ativar o Runtime Monitoring para sua conta ou organização, certifique-se também de configurar o agente de GuardDuty segurança para o recurso que você deseja monitorar para detecção de ameaças. Por exemplo, se você quiser usar o Runtime Monitoring para suas instâncias do Amazon EC2, depois de habilitar o Runtime Monitoring, você também deverá configurar o agente de segurança para o Amazon EC2. Você pode optar por fazer isso manualmente ou automaticamente por meio de GuardDuty.
- O plano de proteção do Runtime Monitoring está ativado no nível da conta. O período de teste gratuito de 30 dias funciona no nível dos recursos. Depois que o agente GuardDuty de segurança é implantado em um tipo de recurso específico, o teste gratuito de 30 dias começa quando GuardDuty recebe seu primeiro evento de tempo de execução associado a esse tipo de recurso. Por exemplo, você implantou o GuardDuty agente no nível do recurso (para a instância do Amazon EC2, o cluster do Amazon ECS e o cluster do Amazon EKS). Quando GuardDuty receber o primeiro evento de tempo de execução de uma instância do Amazon EC2, o teste gratuito de 30 dias começará somente para o Amazon EC2.
- Quando você deseja ativar somente o EKS Runtime Monitoring — Quando você ativa GuardDuty pela primeira vez, o EKS Runtime Monitoring não é ativado por padrão (após o lançamento do Runtime Monitoring). Você precisará ativar o EKS Runtime Monitoring. Para usá-lo de forma ideal, certifique-se de gerenciar o agente de GuardDuty segurança manualmente ou habilitar a configuração automática do agente para que ele GuardDuty gerencie o agente em seu nome. Seu período de teste gratuito de 30 dias do EKS Runtime Monitoring começa quando GuardDuty recebe seu primeiro evento de tempo de execução para o recurso Amazon EKS.

Eu habilitei o EKS Runtime Monitoring antes do lançamento do Runtime Monitoring

- Para uma GuardDuty conta existente que tem o plano de proteção do EKS Runtime Monitoring ativado e usa a experiência do GuardDuty console para usar esse plano de proteção, com o

anúncio do Runtime Monitoring, a experiência do console do EKS Runtime Monitoring agora foi consolidada no Runtime Monitoring. Sua configuração existente para o EKS Runtime Monitoring permanece a mesma. Você pode continuar usando o suporte de API/CLI para realizar operações associadas ao EKS Runtime Monitoring.

- Para usar o EKS Runtime Monitoring como parte do Runtime Monitoring, você precisará configurar o Runtime Monitoring para sua conta ou organização. Para manter a mesma configuração para o Runtime Monitoring, consulteMigração do monitoramento de tempo de execução do EKS para o monitoramento de tempo de execução. No entanto, isso não afetará seu teste gratuito de 30 dias do recurso Amazon EKS.
- O plano de proteção do Runtime Monitoring está ativado no nível da conta. Depois que o agente de GuardDuty segurança é implantado em um dos tipos de recursos especificados (instância do Amazon EC2 e cluster do Amazon ECS), o teste gratuito de 30 dias começa GuardDuty quando recebe o primeiro evento de tempo de execução associado ao recurso. Há um teste gratuito de 30 dias associado a cada tipo de recurso.

  Por exemplo, depois de ativar o Runtime Monitoring, você opta por implantar o GuardDuty agente somente na instância do Amazon EC2. O teste gratuito de 30 dias desse recurso começará somente quando GuardDuty receber seu primeiro evento de tempo de execução para uma instância do Amazon EC2. Posteriormente, quando você implantar o GuardDuty agente para o Fargate (somente Amazon ECS), o teste gratuito de 30 dias desse recurso começará somente quando GuardDuty receber seu primeiro evento de tempo de execução para o cluster Amazon ECS. Considerando que você já tem o EKS Runtime Monitoring ativado para sua conta, GuardDuty não redefine o teste gratuito de 30 dias de um recurso do Amazon EKS.

Pré-requisitos para habilitar o monitoramento de tempo de execução

Para habilitar o Runtime Monitoring e gerenciar o agente de GuardDuty segurança, você deve atender aos pré-requisitos de cada tipo de recurso que deseja monitorar para detecção de ameaças.

Conteúdo

Pré-requisitos para suporte à instância do Amazon EC2

Pré-requisito geral

As instâncias do Amazon EC2 para as quais você deseja monitorar eventos de tempo GuardDuty de execução devem ser gerenciadas por SSM. Isso ocorre independentemente de você usar GuardDuty para gerenciar o agente de segurança automaticamente ou gerenciá-lo manualmente (exceto[Método 2 - Usando scripts de instalação do RPM]).

Para gerenciar suas instâncias do Amazon EC2 com AWS Systems Manager, consulte [Configurando o Systems Manager para instâncias do Amazon EC2] no AWS Systems Manager Guia do usuário.

Validação dos requisitos de arquitetura

A arquitetura da distribuição do sistema operacional pode afetar o comportamento do agente de GuardDuty segurança. Você deve atender aos seguintes requisitos antes de usar o Runtime Monitoring para instâncias do Amazon EC2:

- Atualmente, o suporte do Runtime Monitoring para o Amazon EC2 está disponível somente para versões Linux. Embora o suporte para o Ubuntu não esteja disponível no momento, ele estará em um futuro próximo. Para receber notificações sobre atualizações nesta página, assine o feed RSS.

  A tabela a seguir mostra a distribuição do sistema operacional que foi verificada para oferecer suporte ao agente GuardDuty de segurança para instâncias do Amazon EC2.

Distribuição do sistema operacional	Versão do kernel	Suporte do kernel	Arquitetura da CPU	
			x64 (AMD64)	Graviton (ARM64)
AL2 e AL2023	5.4, 5.10, 5.15, 6.1	eBPF, Tracepoints, Kprobe	Compatível	Compatível

- Requisitos adicionais - Somente se você tiver o Amazon ECS/Amazon EC2

  Para o Amazon ECS/Amazon EC2, recomendamos que você use as AMIs otimizadas para Amazon ECS mais recentes (datadas de 29 de setembro de 2023 ou posterior) ou use a versão v1.77.0 do agente Amazon ECS.

Ao usar a configuração automatizada do agente

Para Use a configuração automatizada do agente (recomendado) isso, você Conta da AWS deve atender aos seguintes pré-requisitos:

- Ao usar tags de inclusão com configuração automática de agentes, GuardDuty para criar uma associação SSM para uma nova instância, certifique-se de que a nova instância seja gerenciada por SSM e apareça no Fleet Manager no console https://console.aws.amazon.com/systems-manager/.
- Ao usar tags de exclusão com a configuração automatizada do agente:
  - Adicione a `false` tag`GuardDutyManaged`: antes de configurar o agente GuardDuty automatizado para sua conta.

    Certifique-se de adicionar a tag de exclusão às suas instâncias do Amazon EC2 antes de iniciá-las. Quando você habilita a configuração automática de agentes para o Amazon EC2, qualquer instância do EC2 que seja executada sem uma tag de exclusão será coberta GuardDuty pela configuração automática do agente.
  - Para que as tags de exclusão funcionem, atualize a configuração da instância para que o documento de identidade da instância esteja disponível no serviço de metadados da instância (IMDS). O procedimento para realizar essa etapa já faz parte da Habilitando o monitoramento de tempo sua conta.

Limite de CPU e memória para o GuardDuty agente

Limite de CPU

O limite máximo de CPU para o agente GuardDuty de segurança associado às instâncias do Amazon EC2 é de 10% do total de núcleos de vCPU. Por exemplo, se sua instância do EC2 tiver 4 núcleos de vCPU, o agente de segurança poderá usar no máximo 40% do total disponível de 400%.

Limite de memória

Da memória associada à sua instância do Amazon EC2, há uma memória limitada que o agente de GuardDuty segurança pode usar.

A tabela a seguir mostra o limite de memória.

Memória da instância do Amazon EC2	Memória máxima para GuardDuty agente
Menos de 8 GB	128 MB
Menos de 32 GB	256 MB
Maior ou igual a 32 GB	1 GB

Próxima etapa

A próxima etapa é configurar o Runtime Monitoring e também gerenciar o agente de segurança (automática ou manualmente). Para ter mais informações, consulte Habilitando o monitoramento de tempo.

Pré-requisitos para suporte (somente para AWS Fargate Amazon ECS)

Validação dos requisitos de arquitetura

A plataforma que você usa pode afetar o suporte do agente GuardDuty de segurança GuardDuty no recebimento de eventos de tempo de execução de seus clusters do Amazon ECS. Você precisa validar que está usando uma das plataformas verificadas.

Considerações iniciais:

- A AWS Fargate (Fargate) plataforma para seus clusters do Amazon ECS deve ser Linux. A versão da plataforma correspondente deve ser pelo menos`1.4.0`, ou`LATEST`. Para obter mais informações sobre as versões da plataforma, consulte as versões da plataforma Linux no Amazon Elastic Container Service Developer Guide.

- As versões da plataforma Windows ainda não são suportadas.

Plataformas verificadas

A distribuição do sistema operacional e a arquitetura da CPU afetam o suporte fornecido pelo agente GuardDuty de segurança. A tabela a seguir mostra a configuração verificada para implantar o agente de GuardDuty segurança e configurar o Runtime Monitoring.

Distribuição do sistema operacional	Suporte do kernel	Arquitetura da CPU

		x64 (AMD64)	Graviton (ARM64)
Linux	eBPF, Tracepoints, Kprobe	Supported	Supported

Forneça permissões de ECR e detalhes da sub-rede

Antes de ativar o Runtime Monitoring, você deve fornecer os seguintes detalhes:

Forneça uma função de execução de tarefas com permissões

A função de execução da tarefa exige que você tenha determinadas permissões do Amazon Elastic Container Registry (Amazon ECR). Você pode usar a política gerenciada do TaskExecutionRolePolicyAmazonECS ou adicionar as seguintes permissões à sua política: `TaskExecutionRole`

```
...
      "ecr:GetAuthorizationToken",
      "ecr:BatchCheckLayerAvailability",
      "ecr:GetDownloadUrlForLayer",
      "ecr:BatchGetImage",
...
```

Para restringir ainda mais as permissões do Amazon ECR, você pode adicionar o URI do repositório do Amazon ECR que hospeda o agente de GuardDuty segurança para (somente AWS Fargate Amazon ECS). Para ter mais informações, consulte Repositório para GuardDuty agente em AWS Fargate (somente Amazon ECS).

Forneça detalhes da sub-rede na definição da tarefa

Você pode fornecer as sub-redes públicas como uma entrada na definição de sua tarefa ou criar um endpoint Amazon ECR VPC.

- Usar a opção de definição de tarefas — Executar as UpdateServiceAPIs CreateServicee no Amazon Elastic Container Service API Reference exige que você passe as informações da sub-rede. Para obter mais informações, consulte as definições de tarefas do Amazon ECS no Amazon Elastic Container Service Developer Guide.
- Usando a opção de endpoint VPC do Amazon ECR — Forneça um caminho de rede para o Amazon ECR — Garanta que o URI do repositório Amazon ECR que GuardDuty hospeda o agente de segurança esteja acessível pela rede. Se suas tarefas do Fargate forem executadas

em uma sub-rede privada, o Fargate precisará do caminho da rede para baixar o contêiner. GuardDuty

Para obter informações sobre como permitir que o Fargate baixe o GuardDuty contêiner, consulte Como usar o Amazon ECR com o Amazon ECS no Guia do desenvolvedor do Amazon Elastic Container Service.

Limites de CPU e memória

Na definição da tarefa do Fargate, você deve especificar o valor da CPU e da memória no nível da tarefa. A tabela a seguir mostra as combinações válidas de valores de CPU e memória em nível de tarefa e o limite máximo de memória do agente de GuardDuty segurança correspondente para o GuardDuty contêiner.

Valor de CPU	Valor de memória	GuardDuty limite máximo de memória do agente
256 (0,25 vCPU)	512 MiB, 1 GB, 2 GB	128 MB
512 (0,5 vCPU)	1 GB, 2 GB, 3 GB, 4 GB	
1024 (1 vCPU)	2 GB, 3 GB, 4 GB	
	5 GB, 6 GB, 7 GB, 8 GB	
2048 (2 vCPU)	Entre 4 GB e 16 GB em incrementos de 1 GB	
4096 (4 vCPU)	Entre 8 GB e 20 GB em incrementos de 1 GB	
8192 (8 vCPU)	Entre 16 GB e 28 GB em incrementos de 4 GB	256 MB
	Entre 32 GB e 60 GB em incrementos de 4 GB	512 MB
16384 (16 vCPU)	Entre 32 GB e 120 GB em incrementos de 8 GB	1 GB

Depois de ativar o Runtime Monitoring e avaliar se o status da cobertura do seu cluster é íntegro, você pode configurar e visualizar as métricas do Container Insight. Para obter mais informações, Configurando o monitoramento no cluster Amazon ECS.

A próxima etapa é configurar o Runtime Monitoring e também gerenciar o agente de segurança. Para ter mais informações, consulte Habilitando o monitoramento de tempo.

Pré-requisitos para suporte ao cluster Amazon EKS

Validação dos requisitos de arquitetura

A plataforma que você usa pode afetar o suporte do GuardDuty Security Agent GuardDuty no recebimento de eventos de tempo de execução de seus clusters EKS. Você precisa validar que está usando uma das plataformas verificadas. Se você estiver gerenciando o GuardDuty agente manualmente, certifique-se de que a versão do Kubernetes seja compatível com a versão do GuardDuty agente que está em uso no momento.

Plataformas verificadas

A distribuição do sistema operacional, a versão do kernel e a arquitetura da CPU afetam o suporte fornecido pelo agente GuardDuty de segurança. A tabela a seguir mostra a configuração verificada para implantar o agente de GuardDuty segurança e configurar o EKS Runtime Monitoring.

Distribuição do sistema operacional	Versão do kernel	Suporte do kernel	Arquitetura da CPU		Versão compatível do Kubernetes
			x64 (AMD64)	Graviton (ARM64) (Graviton2 e superior) 1	
Ubuntu	5.4, 5.10, 5.15, 6.1	eBPF Tracepoints, Kprobe	Compatível	Compatível	v1.21 - v1.29
AL2					
Bottlerocket					v1.23 - v1.29

1.

O monitoramento de tempo de execução para clusters do Amazon EKS não é compatível com a instância Graviton de primeira geração, como os tipos de instância A1.

Versões do Kubernetes suportadas pelo agente de segurança GuardDuty

A tabela a seguir mostra as versões do Kubernetes para seus clusters EKS que são compatíveis com o agente de GuardDuty segurança.

Versão do Kubernetes	Versão complementar do agente de GuardDuty segurança Amazon EKS							
	v1.5.0	v1.4.1	v1.4.0	v1.3.1	v1.3.0	v1.2.0	v1.1.0	v1.0.0
1,29	Compatível	Compatível	Compatível	Não suportado	Não suportado	Não suportado	Não suportado	Sem suporte
1,28				Compatível	Compatível			
1,27						Compatível		
1,26							Compatível	
1,25								Compatível
1,24								
1,23								
1,22								
1,21								

Algumas das versões do agente de GuardDuty segurança chegarão ao fim do suporte padrão. Para obter informações sobre as versões de lançamento do agente, consulteGuardDuty agente de segurança para clusters Amazon EKS.

Limites de CPU e memória

A tabela a seguir mostra os limites de CPU e memória do complemento Amazon EKS para GuardDuty (`aws-guardduty-agent`).

Parâmetro	Limite mínimo	Limite máximo
CPU	200 m	1000 m
Memória	256 Mi	1024 Mi

Quando você usa a versão 1.5.0 ou superior do complemento Amazon EKS, GuardDuty fornece a capacidade de configurar o esquema complementar para seus valores de CPU e memória. Para obter informações sobre o intervalo configurável, consulteParâmetros e valores configuráveis.

Depois de ativar o Monitoramento de runtime do EKS e avaliar o status de cobertura dos seus clusters do EKS, você pode configurar e visualizar as métricas de insights do contêiner. Para ter mais informações, consulte Configurar o monitoramento da CPU e da memória.

Conceitos principais - Abordagens para gerenciar o agente GuardDuty de segurança

Considere os principais conceitos que ajudarão você a gerenciar o agente de segurança em seus clusters Amazon EKS e Amazon ECS.

Conteúdo

- Recurso Fargate (somente Amazon ECS) - Abordagens para gerenciar o agente de segurança GuardDuty
- Clusters do Amazon EKS — Abordagens para gerenciar agentes GuardDuty de segurança

Recurso Fargate (somente Amazon ECS) - Abordagens para gerenciar o agente de segurança GuardDuty

O Runtime Monitoring oferece a opção de detectar possíveis ameaças à segurança em todos os clusters do Amazon ECS (nível de conta) ou em clusters seletivos (nível de cluster) em sua conta. Quando você habilita a configuração automatizada do agente para cada tarefa do Amazon ECS

Fargate que será executada GuardDuty , adicionará um contêiner auxiliar para cada carga de trabalho de contêiner dentro dessa tarefa. O agente GuardDuty de segurança é implantado nesse contêiner auxiliar. É assim que GuardDuty se obtém visibilidade do comportamento em tempo de execução dos contêineres dentro das tarefas do Amazon ECS.

Atualmente, o Runtime Monitoring oferece suporte ao gerenciamento do agente de segurança para seus clusters do Amazon ECS (AWS Fargate) somente por meio de. GuardDuty Não há suporte para gerenciar o agente de segurança manualmente nos clusters do Amazon ECS.

Antes de configurar suas contas, avalie como você deseja gerenciar o agente de GuardDuty segurança e, potencialmente, monitorar o comportamento de tempo de execução dos contêineres que pertencem às tarefas do Amazon ECS. Considere as seguintes abordagens.

Tópicos

Gerencie o agente GuardDuty de segurança para todos os clusters do Amazon ECS

Essa abordagem ajudará você a detectar possíveis ameaças à segurança no nível da conta. Use essa abordagem quando quiser GuardDuty detectar possíveis ameaças de segurança para todos os clusters do Amazon ECS que pertencem à sua conta.

Gerencie o agente de GuardDuty segurança para a maioria dos clusters do Amazon ECS, mas exclua alguns dos clusters do Amazon ECS

Use essa abordagem quando quiser detectar possíveis ameaças GuardDuty à segurança para a maioria dos clusters do Amazon ECS em seu AWS ambiente, mas excluir alguns dos clusters. Essa abordagem ajuda você a monitorar o comportamento de tempo de execução dos contêineres em suas tarefas do Amazon ECS no nível do cluster. Por exemplo, o número de clusters do Amazon ECS que pertencem à sua conta é 1000. No entanto, você deseja monitorar somente 930 clusters do Amazon ECS.

Essa abordagem exige que você adicione uma GuardDuty tag predefinida aos clusters do Amazon ECS que você não deseja monitorar. Para ter mais informações, consulte Gerenciamento de agente de segurança automatizado para Fargate (somente Amazon ECS).

Gerencie o agente GuardDuty de segurança para clusters seletivos do Amazon ECS

Use essa abordagem quando quiser detectar possíveis ameaças GuardDuty à segurança de alguns dos clusters do Amazon ECS. Essa abordagem ajuda você a monitorar o comportamento de tempo de execução dos contêineres em suas tarefas do Amazon ECS no nível do cluster. Por exemplo, o número de clusters do Amazon ECS que pertencem à sua conta é 1000. No entanto, você deseja monitorar somente 230 clusters.

Essa abordagem exige que você adicione uma GuardDuty tag predefinida aos clusters do Amazon ECS que você deseja monitorar. Para ter mais informações, consulte Gerenciamento de agente de segurança automatizado para Fargate (somente Amazon ECS).

Clusters do Amazon EKS — Abordagens para gerenciar agentes GuardDuty de segurança

GuardDuty Para consumir os eventos de tempo de execução de seus clusters EKS no nível da conta ou do cluster, é necessário gerenciar o agente de GuardDuty segurança dos clusters correspondentes.

Abordagens para gerenciar o agente GuardDuty de segurança

Antes de 13 de setembro de 2023, você podia configurar GuardDuty para gerenciar o agente de segurança no nível da conta. Esse comportamento indicou que, por padrão, GuardDuty gerenciará o agente de segurança em todos os clusters EKS que pertencem a um Conta da AWS. Agora, GuardDuty fornece um recurso granular para ajudá-lo a escolher os clusters EKS nos quais você GuardDuty deseja gerenciar o agente de segurança.

Ao escolher Gerencie o agente de GuardDuty segurança manualmente, você ainda pode selecionar os clusters do EKS que deseja monitorar. No entanto, para gerenciar o agente manualmente, criar um endpoint da Amazon VPC para sua Conta da AWS é um pré-requisito.

> **Note**
>
> Independentemente da abordagem usada para gerenciar o agente de GuardDuty segurança, o EKS Runtime Monitoring está sempre ativado no nível da conta.

Tópicos

- Gerencie o agente de segurança por meio de GuardDuty
- Gerencie o agente de GuardDuty segurança manualmente

Gerencie o agente de segurança por meio de GuardDuty

GuardDuty implanta e gerencia o agente de segurança em seu nome. A qualquer momento, você pode monitorar os clusters do EKS em sua conta usando uma das abordagens a seguir.

Tópicos

- Monitorar todos os clusters do EKS
- Monitorar todos os clusters do EKS e excluir clusters do EKS seletivos
- Monitorar clusters do EKS seletivos

Monitorar todos os clusters do EKS

- Quando usar essa abordagem — Use essa abordagem quando quiser GuardDuty implantar e gerenciar o agente de segurança para todos os clusters EKS em sua conta. Por padrão, também GuardDuty implantará o agente de segurança em um cluster EKS potencialmente novo criado em sua conta.
- Impacto do uso dessa abordagem:
  - GuardDuty cria um endpoint da Amazon Virtual Private Cloud (Amazon VPC) por meio do qual o agente de GuardDuty segurança entrega os eventos de tempo de execução. GuardDuty Não há custo adicional para a criação do endpoint Amazon VPC quando você gerencia o agente de segurança por meio de. GuardDuty
  - É necessário que seu nó de trabalho tenha um caminho de rede válido para um `guardduty-data` VPC endpoint ativo. GuardDuty implanta o agente de segurança em seus clusters EKS. O Amazon Elastic Kubernetes Service (Amazon EKS) coordenará a implantação do agente de segurança nos nós dos clusters do EKS.
  - Com base na disponibilidade de IP, GuardDuty seleciona a sub-rede para criar um VPC endpoint. Se você usa topologias de rede avançadas, deve validar se a conectividade é possível.
- Consideração: atualmente, quando você usa essa opção, o Monitoramento de runtime do EKS não cria uma VPC compartilhada.

Monitorar todos os clusters do EKS e excluir clusters do EKS seletivos

- Quando usar essa abordagem — Use essa abordagem quando quiser GuardDuty gerenciar o agente de segurança para todos os clusters EKS em sua conta, mas excluir clusters EKS seletivos. Esse método usa uma abordagem baseada em tags[1] em que é possível marcar os clusters do EKS dos quais não deseja receber os eventos de runtime. A tag predefinida deve ter `GuardDutyManaged-false` como par de chave-valor.
- Impacto do uso dessa abordagem:
  - Essa abordagem exige que você ative o gerenciamento automático do GuardDuty agente somente depois de adicionar tags aos clusters EKS que você deseja excluir do monitoramento.

    Portanto, o impacto ao Gerencie o agente de segurança por meio de GuardDuty também se aplica a essa abordagem. Quando você adiciona tags antes de ativar o gerenciamento automático do GuardDuty agente, não GuardDuty implantará nem gerenciará o agente de segurança para os clusters EKS que estão excluídos do monitoramento.
- Considerações:
  - Você deve adicionar o par de chave-valor da tag como`GuardDutyManaged`: `false` para os clusters EKS seletivos antes de ativar a configuração automatizada do agente, caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS até que você use a tag.
  - Você deve evitar que as tags sejam modificadas, exceto por identidades confiáveis.

    > **Important**
    >
    > Gerencie as permissões para modificar o valor da tag `GuardDutyManaged` para seu cluster do EKS usando políticas de controle de serviço ou políticas do IAM. Para obter mais informações, consulte Políticas de controle de serviços (SCPs) no Guia AWS Organizations do usuário ou Controle o acesso aos AWS recursos no Guia do usuário do IAM.
  - Para um cluster do EKS possivelmente novo que você não deseja monitorar, certifique-se de adicionar o par de chave-valor `GuardDutyManaged-false` no momento da criação desse cluster do EKS.
  - Essa abordagem também terá a mesma consideração especificada para Monitorar todos os clusters do EKS.

Monitorar clusters do EKS seletivos

- Quando usar essa abordagem — Use essa abordagem quando quiser GuardDuty implantar e gerenciar as atualizações do agente de segurança somente para clusters EKS seletivos em sua conta. Esse método usa uma abordagem baseada em tags[1] em que é possível marcar o cluster do EKS do qual deseja receber os eventos de runtime.
- Impacto do uso dessa abordagem:
  - Ao usar tags de inclusão, GuardDuty implantará e gerenciará automaticamente o agente de segurança somente para os clusters EKS seletivos marcados com `GuardDutyManaged - true` como o par de valores-chave.
  - Essa abordagem também terá o mesmo impacto especificado para Monitorar todos os clusters do EKS.
- Considerações:
  - Se o valor da tag `GuardDutyManaged` não estiver definido como `true`, a tag de inclusão não funcionará conforme o esperado e isso pode afetar o monitoramento do seu cluster do EKS.
  - Para garantir que seus clusters do EKS seletivos sejam monitorados, você precisa evitar que as tags sejam modificadas, exceto por identidades confiáveis.

    > **Important**
    >
    > Gerencie as permissões para modificar o valor da tag `GuardDutyManaged` para seu cluster do EKS usando políticas de controle de serviço ou políticas do IAM. Para obter mais informações, consulte Políticas de controle de serviços (SCPs) no Guia AWS Organizations do usuário ou Controle o acesso aos AWS recursos no Guia do usuário do IAM.

  - Para um cluster do EKS possivelmente novo que você não deseja monitorar, certifique-se de adicionar o par de chave-valor `GuardDutyManaged-false` no momento da criação desse cluster do EKS.
  - Essa abordagem também terá a mesma consideração especificada para Monitorar todos os clusters do EKS.

[1]Para obter mais informações sobre a marcação de clusters do EKS seletivos, consulte Como marcar seus recursos do Amazon EKS no Guia do usuário do Amazon EKS.

Gerencie o agente de GuardDuty segurança manualmente

- Quando usar essa abordagem — Use essa abordagem quando quiser implantar e gerenciar o agente de GuardDuty segurança em todos os seus clusters EKS manualmente. Certifique-se de que o Monitoramento de runtime do EKS esteja ativado para suas contas. O agente GuardDuty de segurança pode não funcionar conforme o esperado se você não ativar o EKS Runtime Monitoring.
- Impacto do uso dessa abordagem — Você precisará coordenar a implantação do software do agente de GuardDuty segurança em seus clusters EKS em todas as contas e Regiões da AWS onde esse recurso estiver disponível.
- Considerações: você deve oferecer suporte ao fluxo de dados seguro enquanto monitora e aborda as lacunas de cobertura à medida que novos clusters e workloads são implantados continuamente.

Habilitando o GuardDuty monitoramento de tempo

Antes de ativar o Runtime Monitoring em sua conta, certifique-se de que o tipo de recurso para o qual você deseja monitorar os eventos de tempo de execução seja compatível com os requisitos da plataforma. Para ter mais informações, consulte Pré-requisitos.

Se você usa o EKS Runtime Monitoring antes do lançamento do Runtime Monitoring, pode usar as APIs para verificar e atualizar a configuração existente do EKS Runtime Monitoring. Você também pode migrar sua configuração existente do EKS Runtime Monitoring para o Runtime Monitoring. Para ter mais informações, consulte Migração do monitoramento de tempo de execução do EKS para o monitoramento de tempo de execução.

> **Note**
>
> Atualmente, esta documentação fornece etapas para habilitar o Runtime Monitoring para suas contas e organização somente por console. Você também pode ativar o Runtime Monitoring usando ações de API ou AWS CLI for GuardDuty.

Você pode configurar o Runtime Monitoring usando as etapas nos tópicos a seguir.

Conteúdo

- Gerenciando agentes GuardDuty de segurança

Habilitando o Runtime Monitoring para uma conta independente

Console

1. Faça login no AWS Management Console e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Runtime Monitoring.
3. Na guia Configuração, escolha Habilitar para ativar o monitoramento de tempo de execução para sua conta.
4. GuardDuty Para receber os eventos de tempo de execução de um ou mais tipos de recursos — uma instância do Amazon EC2, um cluster do Amazon ECS ou um cluster do Amazon EKS, use as seguintes opções para gerenciar o agente de segurança desses recursos:

   Para habilitar o agente GuardDuty de segurança

   - Gerenciando o agente de segurança automatizado para a instância do Amazon EC2
   - Gerenciando o agente de segurança manualmente para a instância do Amazon EC2
   - Gerenciamento de agente de segurança automatizado para Fargate (somente Amazon ECS)
   - Gerenciando automaticamente o agente de segurança para clusters do Amazon EKS
   - Gerenciando o agente de segurança manualmente para o cluster Amazon EKS

Para ambientes com várias contas

Em ambientes com várias contas, somente a conta de GuardDuty administrador delegado pode ativar ou desativar o Runtime Monitoring para as contas dos membros e gerenciar a configuração automatizada do agente para os tipos de recursos pertencentes às contas dos membros em sua organização. As contas GuardDuty dos membros não podem modificar essa configuração em suas contas. A conta de GuardDuty administrador delegado gerencia suas contas de membros usando AWS Organizations. Para obter mais informações sobre ambientes com várias contas, consulte Gerenciar de várias contas.

Para conta de GuardDuty administrador delegado

Para habilitar o Runtime Monitoring para uma conta de GuardDuty administrador delegado

1. Faça login no AWS Management Console e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Runtime Monitoring.
3. Na guia Configuração, escolha Editar na seção Configuração do Runtime Monitoring.
4. Como usar a opção Habilitar para todas as contas

   Se você quiser ativar o Runtime Monitoring para todas as contas que pertencem à organização, incluindo a conta de GuardDuty administrador delegado, escolha Habilitar para todas as contas.
5. Como usar a opção Configurar contas manualmente

   Se você quiser ativar o Runtime Monitoring para cada conta de membro individualmente, escolha Configurar contas manualmente.

   - Selecione Habilitar na seção Administrador delegado (esta conta).
6. GuardDuty Para receber os eventos de tempo de execução de um ou mais tipos de recursos — uma instância do Amazon EC2, um cluster do Amazon ECS ou um cluster do Amazon EKS, use as seguintes opções para gerenciar o agente de segurança desses recursos:

   Para habilitar o agente GuardDuty de segurança

   - Gerenciando o agente de segurança automatizado para a instância do Amazon EC2
   - Gerenciando o agente de segurança manualmente para a instância do Amazon EC2
   - Gerenciamento de agente de segurança automatizado para Fargate (somente Amazon ECS)
   - Gerenciando automaticamente o agente de segurança para clusters do Amazon EKS
   - Gerenciando o agente de segurança manualmente para o cluster Amazon EKS

Para todas as contas de membros

Para habilitar o Runtime Monitoring para todas as contas de membros na organização

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

   Faça login usando a conta de GuardDuty administrador delegado.

2. No painel de navegação, escolha Runtime Monitoring.
3. Na página Runtime Monitoring, na guia Configuração, escolha Editar na seção Configuração do Runtime Monitoring.
4. Escolha Habilitar para todas as contas.
5. GuardDuty Para receber os eventos de tempo de execução de um ou mais tipos de recursos — uma instância do Amazon EC2, um cluster do Amazon ECS ou um cluster do Amazon EKS, use as seguintes opções para gerenciar o agente de segurança desses recursos:

   Para habilitar o agente GuardDuty de segurança

   - Gerenciando o agente de segurança automatizado para a instância do Amazon EC2
   - Gerenciando o agente de segurança manualmente para a instância do Amazon EC2
   - Gerenciamento de agente de segurança automatizado para Fargate (somente Amazon ECS)
   - Gerenciando automaticamente o agente de segurança para clusters do Amazon EKS
   - Gerenciando o agente de segurança manualmente para o cluster Amazon EKS

Para todas as contas de membros ativas existentes

Para habilitar o Runtime Monitoring para contas de membros existentes na organização

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

   Faça login usando a conta de GuardDuty administrador delegado da organização.
2. No painel de navegação, escolha Runtime Monitoring.
3. Na página Runtime Monitoring, na guia Configuração, você pode ver o status atual da configuração do Runtime Monitoring.
4. No painel Runtime Monitoring, na seção Contas de membros ativos, escolha Ações.
5. No menu suspenso Ações, escolha Habilitar para todas as contas-membro ativas existentes.
6. Selecione a opção Confirmar.
7. GuardDuty Para receber os eventos de tempo de execução de um ou mais tipos de recursos — uma instância do Amazon EC2, um cluster do Amazon ECS ou um cluster do Amazon EKS, use as seguintes opções para gerenciar o agente de segurança desses recursos:

Para habilitar o agente GuardDuty de segurança

- Gerenciando o agente de segurança automatizado para a instância do Amazon EC2
- Gerenciando o agente de segurança manualmente para a instância do Amazon EC2
- Gerenciamento de agente de segurança automatizado para Fargate (somente Amazon ECS)
- Gerenciando automaticamente o agente de segurança para clusters do Amazon EKS
- Gerenciando o agente de segurança manualmente para o cluster Amazon EKS

> **Note**
>
> Pode levar até 24 horas para atualizar a configuração das contas-membro.

Ative automaticamente o Runtime Monitoring somente para contas de novos membros

Para habilitar o Runtime Monitoring para novas contas de membros em sua organização

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

   Faça login usando a conta de GuardDuty administrador delegado designada da organização.
2. No painel de navegação, escolha Runtime Monitoring
3. Na guia Configuração, escolha Editar na seção Configuração do Runtime Monitoring.
4. Escolha Configurar contas manualmente.
5. Selecione Habilitar automaticamente para novas contas-membro.
6. GuardDuty Para receber os eventos de tempo de execução de um ou mais tipos de recursos — uma instância do Amazon EC2, um cluster do Amazon ECS ou um cluster do Amazon EKS, use as seguintes opções para gerenciar o agente de segurança desses recursos:

   Para habilitar o agente GuardDuty de segurança

   - Gerenciando o agente de segurança automatizado para a instância do Amazon EC2
   - Gerenciando o agente de segurança manualmente para a instância do Amazon EC2
   - Gerenciamento de agente de segurança automatizado para Fargate (somente Amazon ECS)
   - Gerenciando automaticamente o agente de segurança para clusters do Amazon EKS

- Gerenciando o agente de segurança manualmente para o cluster Amazon EKS

Somente para contas seletivas de membros ativos

Para habilitar o Runtime Monitoring para contas individuais de membros ativos

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Faça login usando as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, escolha Accounts (Contas).
3. Na página Contas, revise os valores nas colunas Runtime Monitoring e Manage agent automatically. Esses valores indicam se o Runtime Monitoring e o gerenciamento de GuardDuty agentes estão habilitados ou não habilitados para a conta correspondente.
4. Na tabela Contas, selecione a conta para a qual você deseja ativar o Runtime Monitoring. É possível escolher várias contas ao mesmo tempo.
5. Selecione a opção Confirmar.
6. Selecione Editar planos de proteção. Escolha a ação apropriada.
7. Selecione a opção Confirmar.
8. GuardDuty Para receber os eventos de tempo de execução de um ou mais tipos de recursos — uma instância do Amazon EC2, um cluster do Amazon ECS ou um cluster do Amazon EKS, use as seguintes opções para gerenciar o agente de segurança desses recursos:

   Para habilitar o agente GuardDuty de segurança

   - Gerenciando o agente de segurança automatizado para a instância do Amazon EC2
   - Gerenciando o agente de segurança manualmente para a instância do Amazon EC2
   - Gerenciamento de agente de segurança automatizado para Fargate (somente Amazon ECS)
   - Gerenciando automaticamente o agente de segurança para clusters do Amazon EKS
   - Gerenciando o agente de segurança manualmente para o cluster Amazon EKS

Gerenciando agentes GuardDuty de segurança

Você pode gerenciar o agente de GuardDuty segurança do recurso que deseja monitorar. Se você quiser monitorar mais de um tipo de recurso, certifique-se de gerenciar o GuardDuty agente desse recurso.

> **Important**
>
> Ao trabalhar com o agente de GuardDuty segurança para uma instância do Amazon EC2, você pode instalar e usar o agente no host subjacente dentro de um cluster do Amazon EKS. Se você já tivesse implantado um agente de segurança nesse cluster EKS, o mesmo host poderia ter dois agentes de segurança em execução ao mesmo tempo. Para obter informações sobre como GuardDuty funciona nesse cenário, consulte Lidando com agentes de segurança duplos.

Os tópicos a seguir ajudarão você nas próximas etapas para gerenciar o agente de segurança.

Conteúdo

Usando VPC compartilhada com agentes de segurança automatizados

Quando você escolhe GuardDuty gerenciar o agente de segurança automaticamente, o Runtime Monitoring oferece suporte ao uso de uma VPC compartilhada para Contas da AWS aqueles que pertencem à mesma organização em. AWS Organizations Em seu nome, GuardDuty você pode definir a política de endpoint da Amazon VPC com base nos detalhes associados à VPC compartilhada da sua organização.

Antes dessa versão, dava GuardDuty suporte ao uso de VPCs compartilhadas somente quando você optava por gerenciar o agente GuardDuty de segurança manualmente.

Conteúdo

Como funcionam

Quando a conta do proprietário da VPC compartilhada ativa o Runtime Monitoring e a configuração automática do agente para qualquer um dos recursos (Amazon EKS ou (somente AWS Fargate Amazon ECS)), todas as VPCs compartilhadas se tornam elegíveis para a instalação automática do endpoint compartilhado da Amazon VPC e do grupo de segurança associado na conta do proprietário da VPC compartilhada. GuardDuty recupera o ID da organização que está associado à Amazon VPC compartilhada.

Agora, aqueles Contas da AWS que pertencem à mesma organização da conta compartilhada do proprietário da Amazon VPC também podem compartilhar o mesmo endpoint da Amazon VPC. GuardDuty cria a VPC compartilhada quando a conta compartilhada do proprietário da VPC ou a conta participante precisam de um endpoint da Amazon VPC. Exemplos de necessidade de um endpoint do Amazon VPC incluem GuardDuty habilitar o Runtime Monitoring, o EKS Runtime Monitoring ou o lançamento de uma nova tarefa do Amazon ECS-Fargate. Quando essas contas habilitam o Runtime Monitoring e a configuração automática de agentes para qualquer tipo de recurso, GuardDuty cria um endpoint da Amazon VPC e define a política de endpoint com o mesmo ID de organização da conta compartilhada do proprietário da VPC. GuardDuty adiciona uma `GuardDutyManaged` tag e a define `true` para o endpoint da Amazon VPC que cria. GuardDuty Se a conta compartilhada do proprietário da Amazon VPC não tiver habilitado o Runtime Monitoring ou a configuração automatizada do agente para nenhum dos recursos, não GuardDuty definirá a política de endpoint da Amazon VPC. Para obter informações sobre como configurar o Runtime Monitoring e gerenciar automaticamente o agente de segurança na conta compartilhada do proprietário da VPC, consulte. Habilitando o GuardDuty monitoramento de tempo

Cada uma das contas que usam a mesma política de endpoint da Amazon VPC é chamada de AWS conta participante da Amazon VPC compartilhada associada.

O exemplo a seguir mostra a política padrão de VPC endpoint da conta compartilhada do proprietário da VPC e da conta do participante. `aws:PrincipalOrgID`Mostrará o ID da organização associado ao recurso VPC compartilhado. O uso desta política é limitado às contas de participantes presentes na organização da conta do proprietário.

Example

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

```
            "Resource": "*",
            "Effect": "Allow",
            "Principal": "*"
        },
        {
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalOrgID": "o-abcdef0123"
                }
            },
            "Action": "*",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "*"
        }
    ]
}
```

Pré-requisitos para usar a VPC compartilhada

Pré-requisitos para a configuração inicial

Execute as seguintes etapas na Conta da AWS qual você deseja ser o proprietário da VPC compartilhada:

1. Criação de uma organização — Crie uma organização seguindo as etapas em Criação e gerenciamento de uma organização no Guia AWS Organizations do usuário.

   Para obter informações sobre como adicionar ou remover contas de membros, consulte Gerenciamento Contas da AWS na sua organização.
2. Criação de um recurso de VPC compartilhado — Você pode criar um recurso de VPC compartilhado a partir da conta do proprietário. Para obter informações, consulte Compartilhar sua VPC com outras contas no Guia do usuário da Amazon VPC.

Pré-requisitos específicos para o monitoramento de tempo de execução GuardDuty

A lista a seguir fornece os pré-requisitos específicos para: GuardDuty

- A conta do proprietário da VPC compartilhada e a conta participante podem ser de diferentes organizações em. GuardDuty No entanto, eles devem pertencer à mesma organização em AWS Organizations. Isso é necessário GuardDuty para criar um endpoint da Amazon VPC e um

grupo de segurança para a VPC compartilhada. Para obter informações sobre como as VPCs compartilhadas funcionam, consulte Compartilhe sua VPC com outras contas no Guia do usuário da Amazon VPC.

- Ative o Runtime Monitoring ou o EKS Runtime Monitoring e a configuração GuardDuty automatizada do agente para qualquer recurso na conta compartilhada do proprietário da VPC e na conta do participante. Para ter mais informações, consulte Habilitando o monitoramento de tempo.

  Se você já tiver concluído essas configurações, continue com a próxima etapa.
- Ao trabalhar com uma tarefa do Amazon EKS ou do Amazon ECS (AWS Fargate somente), certifique-se de escolher o recurso VPC compartilhado associado à conta do proprietário e selecionar suas sub-redes.

Perguntas frequentes (FAQs)

A lista a seguir fornece as etapas de solução de problemas para as perguntas mais frequentes ao usar um recurso de VPC compartilhado com a configuração GuardDuty automatizada do agente habilitada no Runtime Monitoring:

Já estou usando o Runtime Monitoring (ou EKS Runtime Monitoring). Como faço para habilitar a VPC compartilhada?

Para obter informações sobre os pré-requisitos para criar uma VPC compartilhada, consulte. Pré-requisitos

Quando a conta compartilhada do proprietário da VPC e a conta do participante atenderem aos pré-requisitos, GuardDuty tentará definir a política de endpoint da Amazon VPC automaticamente.

Se antes desta versão, você Conta da AWS teve um problema de cobertura sobre a VPC compartilhada não ser suportada, siga os pré-requisitos. Quando seu tipo de recurso (tarefa do Amazon EKS ou do Amazon ECS (AWS Fargate somente)) invoca a exigência de um VPC endpoint compartilhado, GuardDuty tentará definir a nova política de VPC endpoint.

Como uma conta de proprietário de VPC compartilhada, quero que a política de endpoint de VPC compartilhada seja restrita a um subconjunto de contas participantes em minha organização. Como posso fazer isso?

Se você tiver uma `true` tag`GuardDutyManaged`: associada ao endpoint, remova-a. Isso impede GuardDuty a tentativa de modificar ou substituir a política de VPC endpoint da VPC compartilhada.

Para obter mais informações, consulte Controlar o acesso a endpoints de VPC usando políticas de endpoint.

Por que o VPC endpoint compartilhado é modificado de para? **`aws:PrincipalAccountaws:PrincipalOrgId`** Como posso evitar isso?

Quando GuardDuty detecta que a VPC é compartilhada por várias contas da mesma organização AWS Organizations em GuardDuty , tenta modificar a política para especificar o ID da organização.

Para evitar isso, remova a `true` tag`GuardDutyManaged`: do VPC endpoint compartilhado. Isso impede GuardDuty a tentativa de modificar ou substituir a política de VPC endpoint da VPC compartilhada.

O que acontece quando a conta compartilhada do proprietário da VPC ou uma das contas dos participantes desativa o Runtime Monitoring (GuardDuty ou EKS Runtime Monitoring)?

Quando a conta compartilhada do proprietário da VPC desativa GuardDuty o Runtime Monitoring (ou EKS Runtime Monitoring), GuardDuty verifica se algum tipo de recurso pertencente à conta do participante usou o endpoint compartilhado da VPC ou se alguma conta do participante já habilitou o gerenciamento de GuardDuty agentes para qualquer tipo de recurso. Se sim, GuardDuty não excluirá o VPC endpoint e o grupo de segurança.

Se a conta compartilhada do participante da VPC desabilitar GuardDuty o Runtime Monitoring (ou EKS Runtime Monitoring), não haverá impacto na conta compartilhada do proprietário da VPC e a conta do proprietário não excluirá o recurso da VPC compartilhada nem o grupo de segurança.

Como posso excluir o recurso de VPC compartilhado? Qual será seu impacto?

Como uma conta de proprietário de VPC compartilhada, você pode excluir o recurso de VPC compartilhado mesmo quando ele estiver sendo usado por sua conta ou por qualquer uma das contas participantes do Runtime Monitoring. Para obter informações sobre como excluir a VPC compartilhada e entender seu impacto, consulte. To delete VPC endpoint

Lidando com agentes de segurança duplos instalados em um host

As instâncias do Amazon EC2 podem suportar vários tipos de cargas de trabalho. Quando você configura um agente de segurança automatizado em uma instância do Amazon EC2, a mesma instância do EC2 pode ter outro agente de segurança por meio do EKS.

Visão geral

Considere um cenário em que você tenha ativado o Runtime Monitoring. Agora, você habilita o agente automatizado para o Amazon EKS por meio de GuardDuty. Você também habilitou o agente automatizado para o Amazon EC2. Pode acontecer que o mesmo host subjacente seja instalado com dois agentes de segurança: um para o Amazon EKS e outro para o Amazon EC2. Isso pode resultar em dois agentes de segurança funcionando dentro do mesmo host, coletando eventos de tempo de execução e enviando-os para GuardDuty, e potencialmente gerando descobertas duplicadas.

Impacto

- Quando há mais de um agente de segurança em execução no mesmo host, sua conta pode ter o dobro das necessidades de processamento de CPU e memória. Para obter informações sobre os limites de CPU e memória para cada tipo de recurso, consulte Pré-requisitos esse recurso.
- GuardDuty projetou o recurso Runtime Monitoring de forma que, mesmo que haja uma sobreposição de dois agentes de segurança coletando eventos de tempo de execução do mesmo host subjacente, sua conta será cobrada apenas por um fluxo de eventos de tempo de execução.

Como GuardDuty lida com vários agentes

GuardDuty detecta quando dois agentes de segurança estão sendo executados no mesmo host e designa somente um deles como o agente de segurança que coleta ativamente os eventos de tempo de execução. O segundo agente consumirá recursos mínimos do sistema para evitar qualquer impacto no desempenho de seus aplicativos.

GuardDuty considera os seguintes cenários:

- Quando uma instância do EC2 se enquadra no escopo dos agentes de segurança do Amazon EKS e do Amazon EC2, o agente de segurança EKS tem prioridade. Isso se aplicará somente quando você usar o agente de segurança v1.1.0 ou superior para o Amazon EC2. As versões mais antigas do agente continuarão sendo executadas e coletando eventos de tempo de execução porque as versões mais antigas do agente não são afetadas pela priorização.
- Quando o Amazon EKS e o Amazon EC2 tiverem agentes de segurança GuardDuty gerenciados e sua instância do Amazon EC2 também for gerenciada por SSM, os dois agentes de segurança serão instalados no nível do host. Depois que os agentes estiverem instalados, GuardDuty decide qual agente de segurança continuará em execução. Quando os dois agentes de segurança estão em execução, eventualmente, apenas um deles coletará eventos de tempo de execução.

- Quando os agentes de segurança associados ao EC2 e ao EKS são executados ao mesmo tempo, GuardDuty podem gerar descobertas duplicadas somente durante o período de sobreposição.

  Isso pode acontecer quando:

  - Os agentes de segurança do EC2 e do EKS são configurados por meio de GuardDuty (automaticamente) ou
  - Seu recurso Amazon EKS tem um agente de segurança automatizado.
- Quando o agente de segurança EKS já estiver em execução, se você implantar o agente de segurança EC2 manualmente no mesmo host subjacente e atender a todos os pré-requisitos, GuardDuty talvez não instale um segundo agente de segurança.

Gerenciando o agente de segurança automatizado para a instância do Amazon EC2

Migração do agente manual do Amazon EC2 para o agente automatizado

Esta seção se aplica Conta da AWS se você já gerenciava o agente de segurança manualmente e agora deseja usar a configuração GuardDuty automatizada do agente. Se isso não se aplicar a você, continue configurando o agente de segurança da sua conta.

Quando você ativa o agente GuardDuty automatizado, GuardDuty gerencia o agente de segurança em seu nome. Para obter informações sobre quais etapas são GuardDuty necessárias, consulteUse a configuração automatizada do agente (recomendado).

Limpeza de recursos

Excluir associação SSM

- Exclua qualquer associação SSM que você possa ter criado ao gerenciar manualmente o agente de segurança do Amazon EC2. Para obter mais informações, consulte Excluindo associações.
- Isso é feito para que GuardDuty possa assumir o gerenciamento das ações de SSM, independentemente de você usar agentes automatizados no nível da conta ou da instância (usando tags de inclusão ou exclusão). Para obter mais informações sobre quais ações do SSM podem ser GuardDuty tomadas, consultePermissões de função vinculadas ao serviço para GuardDuty.
- Quando você exclui uma associação de SSM que foi criada anteriormente para gerenciar o agente de segurança manualmente, pode haver um breve período de sobreposição ao GuardDuty criar uma associação de SSM para gerenciar o agente de segurança

automaticamente. Durante esse período, você pode enfrentar conflitos com base no agendamento do SSM. Para obter mais informações, consulte Programação de SSM do Amazon EC2.

Gerencie tags de inclusão e exclusão para suas instâncias do Amazon EC2

- Tags de inclusão — Quando você não ativa a configuração GuardDuty automática do agente, mas marca qualquer uma das suas instâncias do Amazon EC2 com uma tag de inclusão (`GuardDutyManaged:true`), GuardDuty cria uma associação SSM que instalará e gerenciará o agente de segurança nas instâncias do EC2 selecionadas. Esse é um comportamento esperado que ajuda você a gerenciar o agente de segurança somente em instâncias EC2 selecionadas. Para ter mais informações, consulte Como o Runtime Monitoring funciona com instâncias do Amazon EC2.

  Para GuardDuty evitar a instalação e o gerenciamento do agente de segurança, remova a tag de inclusão dessas instâncias do EC2. Para obter mais informações, consulte Adicionar e excluir tags no Guia do usuário do Amazon EC2 para instâncias Linux.
- Tags de exclusão — Quando você quiser habilitar a configuração GuardDuty automatizada do agente para todas as instâncias do EC2 em sua conta, certifique-se de que nenhuma instância do EC2 esteja marcada com uma tag de exclusão (:). `GuardDutyManaged false`

Configurando o GuardDuty agente para uma conta independente

Configure for all instances

Para configurar o agente GuardDuty de segurança para todas as instâncias em sua conta independente

1. Faça login no AWS Management Console e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Runtime Monitoring.
3. Na guia Configuração, escolha Editar.
4. Na seção EC2, escolha Ativar.
5. Selecione Salvar.
6. Você pode verificar se a associação SSM GuardDuty criada instalará e gerenciará o agente de segurança em todos os recursos do EC2 pertencentes à sua conta.

a. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.

b. Abra a guia Alvos da associação SSM (`GuardDutyRuntimeMonitoring-do-not-delete`). Observe que a chave Tag aparece como InstanceIds.

Using inclusion tag in selected instances

Para configurar o agente GuardDuty de segurança para instâncias selecionadas do Amazon EC2

1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Adicione a `true` tag`GuardDutyManaged`: às instâncias que você GuardDuty deseja monitorar e detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.
3. Você pode verificar se a associação SSM GuardDuty criada instalará e gerenciará o agente de segurança somente nos recursos do EC2 que estão marcados com as tags de inclusão.

   Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.

   - Abra a guia Destinos da associação SSM que é criada (`GuardDutyRuntimeMonitoring-do-not-delete`). A chave Tag aparece como tag: GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Certifique-se de adicionar a tag de exclusão às suas instâncias do Amazon EC2 antes de iniciá-las. Quando você habilita a configuração automática de agentes para o Amazon EC2, qualquer instância do EC2 que seja executada sem uma tag de exclusão será coberta GuardDuty pela configuração automática do agente.

Para configurar o agente GuardDuty de segurança para instâncias selecionadas do Amazon EC2

1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Adicione a `false` tag`GuardDutyManaged`: às instâncias que você não GuardDuty deseja monitorar e detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.
3. Para que as tags de exclusão estejam disponíveis nos metadados da instância, execute as seguintes etapas:

   a. Na guia Detalhes da sua instância, veja o status de Permitir tags nos metadados da instância.

      Se estiver desativado no momento, use as etapas a seguir para alterar o status para Ativado. Caso contrário, ignore essa etapa.

   b. Selecione a instância para a qual você deseja permitir tags.

   c. No menu Ações, escolha Configurações da instância.

   d. Escolha Permitir tags nos metadados da instância.

   e. Em Acesso às tags nos metadados da instância, selecione Permitir.

   f. Selecione Salvar.
4. Depois de adicionar a tag de exclusão, execute as mesmas etapas especificadas na guia Configurar para todas as instâncias.

Agora você pode avaliar o tempo de execuçãoCobertura para a instância do Amazon EC2.

Configurando o GuardDuty agente em um ambiente de várias contas

Para conta de GuardDuty administrador delegado

Configure for all instances

Se você escolher Habilitar para todas as contas do Runtime Monitoring, escolha uma das seguintes opções para a conta de GuardDuty administrador delegado:

- Opção 1

  Em Configuração automatizada do agente, na seção EC2, selecione Habilitar para todas as contas.

- Opção 2
  - Em Configuração automatizada do agente, na seção EC2, selecione Configurar contas manualmente.
  - Em Administrador delegado (esta conta), escolha Habilitar.
- Selecione Salvar.

Se você escolheu Configurar contas manualmente para o Runtime Monitoring, execute as seguintes etapas:

- Em Configuração automatizada do agente, na seção EC2, selecione Configurar contas manualmente.
- Em Administrador delegado (esta conta), escolha Habilitar.
- Selecione Salvar.

Independentemente da opção escolhida para habilitar a configuração automatizada do agente para a conta de GuardDuty administrador delegado, você pode verificar se a associação SSM GuardDuty criada instalará e gerenciará o agente de segurança em todos os recursos do EC2 pertencentes a essa conta.

1. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.
2. Abra a guia Alvos da associação SSM (`GuardDutyRuntimeMonitoring-do-not-delete`). Observe que a chave Tag aparece como InstanceIds.

Using inclusion tag in selected instances

Para configurar o GuardDuty agente para instâncias selecionadas do Amazon EC2

1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Adicione a `true` tag`GuardDutyManaged`: às instâncias que você GuardDuty deseja monitorar e detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.

Adicionar essa tag permitirá GuardDuty instalar e gerenciar o agente de segurança para essas instâncias EC2 selecionadas. Você não precisa habilitar explicitamente a configuração automatizada do agente.

3. Você pode verificar se a associação SSM GuardDuty criada instalará e gerenciará o agente de segurança somente nos recursos do EC2 que estão marcados com as tags de inclusão.

   Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.

   - Abra a guia Destinos da associação SSM que é criada (`GuardDutyRuntimeMonitoring-do-not-delete`). A chave Tag aparece como tag: GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Certifique-se de adicionar a tag de exclusão às suas instâncias do Amazon EC2 antes de iniciá-las. Quando você habilita a configuração automática de agentes para o Amazon EC2, qualquer instância do EC2 que seja executada sem uma tag de exclusão será coberta GuardDuty pela configuração automática do agente.

Para configurar o GuardDuty agente para instâncias selecionadas do Amazon EC2

1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Adicione a `false` tag`GuardDutyManaged`: às instâncias que você não GuardDuty deseja monitorar e detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.
3. Para que as tags de exclusão estejam disponíveis nos metadados da instância, execute as seguintes etapas:

   a. Na guia Detalhes da sua instância, veja o status de Permitir tags nos metadados da instância.

Se estiver desativado no momento, use as etapas a seguir para alterar o status para Ativado. Caso contrário, ignore essa etapa.

b. No menu Ações, escolha Configurações da instância.

c. Escolha Permitir tags nos metadados da instância.

4. Depois de adicionar a tag de exclusão, execute as mesmas etapas especificadas na guia Configurar para todas as instâncias.

Agora você pode avaliar o tempo de execuçãoCobertura para a instância do Amazon EC2.

Ativação automática para todas as contas de membros

> **Note**
>
> Pode levar até 24 horas para atualizar a configuração das contas-membro.

Configure for all instances

As etapas a seguir pressupõem que você tenha escolhido Habilitar para todas as contas na seção Runtime Monitoring:

1. Escolha Habilitar para todas as contas na seção Configuração automática de agentes do Amazon EC2.
2. Você pode verificar se a associação SSM que GuardDuty cria (`GuardDutyRuntimeMonitoring-do-not-delete`) instalará e gerenciará o agente de segurança em todos os recursos do EC2 pertencentes a essa conta.

   a. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.

   b. Abra a guia Alvos da associação SSM. Observe que a chave Tag aparece como InstanceIds.

Using inclusion tag in selected instances

Para configurar o GuardDuty agente para instâncias selecionadas do Amazon EC2

1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Adicione a `true` tag`GuardDutyManaged`: às instâncias do EC2 que você GuardDuty deseja monitorar e detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.

   Adicionar essa tag permitirá GuardDuty instalar e gerenciar o agente de segurança para essas instâncias EC2 selecionadas. Você não precisa habilitar explicitamente a configuração automatizada do agente.
3. Você pode verificar se a associação SSM GuardDuty criada instalará e gerenciará o agente de segurança em todos os recursos do EC2 pertencentes à sua conta.

   a. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.

   b. Abra a guia Alvos da associação SSM (`GuardDutyRuntimeMonitoring-do-not-delete`). Observe que a chave Tag aparece como InstanceIds.

Using exclusion tag in selected instances

> **Note**
>
> Certifique-se de adicionar a tag de exclusão às suas instâncias do Amazon EC2 antes de iniciá-las. Quando você habilita a configuração automática de agentes para o Amazon EC2, qualquer instância do EC2 que seja executada sem uma tag de exclusão será coberta GuardDuty pela configuração automática do agente.

Para configurar o agente GuardDuty de segurança para instâncias selecionadas do Amazon EC2

1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Adicione a `false` tag`GuardDutyManaged`: às instâncias que você não GuardDuty deseja monitorar e detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.

3. Para que as tags de exclusão estejam disponíveis nos metadados da instância, execute as seguintes etapas:

   a. Na guia Detalhes da sua instância, veja o status de Permitir tags nos metadados da instância.

      Se estiver desativado no momento, use as etapas a seguir para alterar o status para Ativado. Caso contrário, ignore essa etapa.

   b. No menu Ações, escolha Configurações da instância.

   c. Escolha Permitir tags nos metadados da instância.

4. Depois de adicionar a tag de exclusão, execute as mesmas etapas especificadas na guia Configurar para todas as instâncias.

Agora você pode avaliar o tempo de execuçãoCobertura para a instância do Amazon EC2.

Ativação automática somente para contas de novos membros

A conta de GuardDuty administrador delegado pode definir a configuração automática do agente para o recurso Amazon EC2 para habilitar automaticamente as novas contas membros à medida que elas ingressam na organização.

Configure for all instances

As etapas a seguir pressupõem que você selecionou Ativar automaticamente para novas contas de membros na seção Monitoramento de tempo de execução:

1. No painel de navegação, escolha Runtime Monitoring.
2. Na página Runtime Monitoring, escolha Editar.
3. Selecione Habilitar automaticamente para novas contas-membro. Essa etapa garante que sempre que uma nova conta ingressar na sua organização, a configuração automática do agente para o Amazon EC2 seja habilitada automaticamente para sua conta. Somente a conta de GuardDuty administrador delegado da organização pode modificar essa seleção.
4. Selecione Salvar.

Quando uma nova conta de membro ingressa na organização, essa configuração será ativada automaticamente para eles. GuardDuty Para gerenciar o agente de segurança das instâncias

do Amazon EC2 que pertencem a essa nova conta membro, certifique-se de que todos os pré-requisitos Para instância EC2 sejam atendidos.

Quando uma associação de SSM é criada (`GuardDutyRuntimeMonitoring-do-not-delete`), você pode verificar se a associação de SSM instalará e gerenciará o agente de segurança em todas as instâncias do EC2 pertencentes à nova conta membro.

- Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.
- Abra a guia Alvos da associação SSM. Observe que a chave Tag aparece como InstanceIds.

Using inclusion tag in selected instances

Para configurar o agente GuardDuty de segurança para instâncias selecionadas em sua conta

1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Adicione a `true` tag`GuardDutyManaged`: às instâncias que você GuardDuty deseja monitorar e detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.

   Adicionar essa tag permitirá GuardDuty instalar e gerenciar o agente de segurança para essas instâncias selecionadas. Você não precisa habilitar explicitamente a configuração automatizada do agente.
3. Você pode verificar se a associação SSM GuardDuty criada instalará e gerenciará o agente de segurança somente nos recursos do EC2 que estão marcados com as tags de inclusão.

   a. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.

   b. Abra a guia Targets da associação SSM que é criada. A chave Tag aparece como tag: GuardDutyManaged.

Using exclusion tag in selected instances

> **Note**
>
> Certifique-se de adicionar a tag de exclusão às suas instâncias do Amazon EC2 antes de iniciá-las. Quando você habilita a configuração automática de agentes para o Amazon

EC2, qualquer instância do EC2 que seja executada sem uma tag de exclusão será coberta GuardDuty pela configuração automática do agente.

Para configurar o agente GuardDuty de segurança para instâncias específicas em sua conta independente

1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Adicione a `false` tag`GuardDutyManaged`: às instâncias que você não GuardDuty deseja monitorar e detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.
3. Para que as tags de exclusão estejam disponíveis nos metadados da instância, execute as seguintes etapas:

   a. Na guia Detalhes da sua instância, veja o status de Permitir tags nos metadados da instância.

      Se estiver desativado no momento, use as etapas a seguir para alterar o status para Ativado. Caso contrário, ignore essa etapa.

   b. No menu Ações, escolha Configurações da instância.

   c. Escolha Permitir tags nos metadados da instância.
4. Depois de adicionar a tag de exclusão, execute as mesmas etapas especificadas na guia Configurar para todas as instâncias.

Agora você pode avaliar o tempo de execuçãoCobertura para a instância do Amazon EC2.

Somente contas seletivas de membros

Configure for all instances

1. Na página Contas, selecione uma ou mais contas para as quais você deseja habilitar a configuração do agente Runtime Monitoring-Automated (Amazon EC2). Certifique-se de que as contas selecionadas nesta etapa já tenham o Runtime Monitoring ativado.
2. Em Editar planos de proteção, escolha a opção apropriada para ativar a configuração automática do agente Runtime Monitoring-Automated (Amazon EC2).
3. Selecione a opção Confirmar.

Using inclusion tag in selected instances

Para configurar o agente GuardDuty de segurança para instâncias selecionadas

1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Adicione a `true` tag`GuardDutyManaged`: às instâncias que você GuardDuty deseja monitorar e detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.

   Adicionar essa tag permitirá GuardDuty gerenciar o agente de segurança para suas instâncias marcadas do Amazon EC2. Você não precisa habilitar explicitamente a configuração automatizada do agente (Runtime Monitoring - Automated Agent Configuration (EC2).

Using exclusion tag in selected instances

> **Note**
>
> Certifique-se de adicionar a tag de exclusão às suas instâncias do Amazon EC2 antes de iniciá-las. Quando você habilita a configuração automática de agentes para o Amazon EC2, qualquer instância do EC2 que seja executada sem uma tag de exclusão será coberta GuardDuty pela configuração automática do agente.

Para configurar o agente GuardDuty de segurança para instâncias selecionadas

1. Faça login no AWS Management Console e abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Adicione a `false` tag`GuardDutyManaged`: às instâncias do EC2 que você não GuardDuty deseja monitorar ou detectar possíveis ameaças. Para obter informações sobre como adicionar essa tag, consulte Para adicionar uma tag a um recurso individual.
3. Para que as tags de exclusão estejam disponíveis nos metadados da instância, execute as seguintes etapas:

   a. Na guia Detalhes da sua instância, veja o status de Permitir tags nos metadados da instância.

Se estiver desativado no momento, use as etapas a seguir para alterar o status para Ativado. Caso contrário, ignore essa etapa.

b. No menu Ações, escolha Configurações da instância.

c. Escolha Permitir tags nos metadados da instância.

4. Depois de adicionar a tag de exclusão, execute as mesmas etapas especificadas na guia Configurar para todas as instâncias.

Agora você pode avaliarCobertura para a instância do Amazon EC2.

Gerenciando o agente de segurança manualmente para a instância do Amazon EC2

Depois de ativar o Runtime Monitoring, você precisará instalar o agente GuardDuty de segurança manualmente. Ao instalar o agente, GuardDuty receberá os eventos de tempo de execução das instâncias do Amazon EC2.

Para gerenciar o agente GuardDuty de segurança, você deve criar um endpoint da Amazon VPC e seguir as etapas para instalar o agente de segurança manualmente.

Criação manual do endpoint Amazon VPC

Antes de instalar o agente de GuardDuty segurança, você deve criar um endpoint da Amazon Virtual Private Cloud (Amazon VPC). Isso ajudará a GuardDuty receber os eventos de tempo de execução de suas instâncias do Amazon EC2.

> **Note**
>
> Não há custo adicional para o uso do VPC endpoint.

Para criar um endpoint Amazon VPC

1. Faça login AWS Management Console e abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, em VPC private cloud, escolha Endpoints.
3. Escolha Criar endpoint.
4. Na página Criar endpoint, para a Categoria de serviço, escolha Outros serviços de endpoint.
5. Em Nome do serviço, digite **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**.

Certifique-se de substituir *us-east-1* pelo seu. Região da AWS Essa deve ser a mesma região da instância do Amazon EC2 que pertence ao ID da sua AWS conta.

6. Selecione Verificar serviço.

7. Depois que o nome do serviço for verificado com sucesso, escolha a VPC em que sua instância reside. Adicione a política a seguir para restringir o uso do endpoint Amazon VPC somente à conta especificada. Com a `Condition` da organização fornecida abaixo desta política, você pode atualizar a política a seguir para restringir o acesso ao seu endpoint. Para fornecer suporte ao endpoint da Amazon VPC para IDs de contas específicas em sua organização, consulte. [Organization condition to restrict access to your endpoint]

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
   "Principal": "*"
  }
 ]
}
```

O ID de conta `aws:PrincipalAccount` deve corresponder à conta que contém a VPC e o endpoint da VPC. A lista a seguir mostra como compartilhar o VPC endpoint com outros AWS IDs de conta:

- Para especificar várias contas para acessar o VPC endpoint, `"aws:PrincipalAccount: "111122223333"` substitua pelo seguinte bloco:

```
"aws:PrincipalAccount": [
          "666666666666",
          "555555555555"
      ]
```

Certifique-se de substituir os AWS IDs da conta pelos IDs das contas que precisam acessar o VPC endpoint.

- Para permitir que todos os membros de uma organização acessem o VPC endpoint, `"aws:PrincipalAccount: "111122223333"` substitua pela seguinte linha:

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

Certifique-se de substituir a organização *o-abcdef0123* pela ID da sua organização.

- Para restringir o acesso a um recurso por meio de um ID da organização, adicione o seu `ResourceOrgID` à política. Para obter mais informações, consulte`aws:ResourceOrgID` no Guia do usuário do IAM.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. Em Configurações adicionais, selecione Habilitar nome DNS.
9. Em Sub-redes, escolha as sub-redes nas quais sua instância reside.
10. Em Grupos de segurança, escolha um grupo de segurança que tenha a porta de entrada 443 habilitada em sua VPC (ou sua instância do Amazon EC2). Se você ainda não tem um grupo de segurança que tenha uma porta de entrada 443 habilitada, consulte Criar um grupo de segurança no Guia do usuário do Amazon EC2 para instâncias Linux.

    Se houver algum problema ao restringir as permissões de entrada para sua VPC (ou instância), forneça suporte à porta 443 de entrada de qualquer endereço IP. (`0.0.0.0/0`)

Instalando o agente de segurança manualmente

GuardDuty fornece os dois métodos a seguir para instalar o agente GuardDuty de segurança em suas instâncias do Amazon EC2:

- Método 1 - Usando AWS Systems Manager — Esse método exige que sua instância do Amazon EC2 seja AWS Systems Manager gerenciada.

- Método 2 - Usando scripts de instalação RPM — Você pode usar esse método independentemente de suas instâncias do Amazon EC2 serem AWS Systems Manager gerenciadas ou não.

Método 1 - Usando AWS Systems Manager

Para usar esse método, certifique-se de que suas instâncias do Amazon EC2 sejam AWS Systems Manager gerenciadas e, em seguida, instale o agente.

AWS Systems Manager instância gerenciada do Amazon EC2

Use as etapas a seguir para gerenciar suas instâncias AWS Systems Manager do Amazon EC2.

- AWS Systems Managerajuda você a gerenciar seus AWS aplicativos e recursos end-to-end e possibilitar operações seguras em grande escala.

  Para gerenciar suas instâncias do Amazon EC2 com AWS Systems Manager, consulte Configurando o Systems Manager para instâncias do Amazon EC2 no AWS Systems Manager Guia do usuário.
- A tabela a seguir mostra os novos AWS Systems Manager documentos GuardDuty gerenciados:

Nome do documento	Tipo de documento	Finalidade
`AmazonGuardDuty-RuntimeMonitoringSsmPlugin`	Distributor	Para empacotar o agente GuardDuty de segurança.
`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`	Command	Para executar o script de instalação/desinstalação para instalar o agente de segurança. GuardDuty

Para obter mais informações sobre AWS Systems Manager, consulte os documentos do Amazon EC2 Systems Manager no Guia AWS Systems Manager do usuário.

Para instalar o GuardDuty agente para a instância do Amazon EC2 usando AWS Systems Manager

1. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.

2. No painel de navegação, escolha Documentos
3. Em Propriedade da Amazon, escolha`AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`.
4. Escolha Run Command.
5. Insira os seguintes parâmetros de execução do comando

   - Ação: Escolha Instalar.
   - Tipo de instalação: Escolha Instalar ou Desinstalar.
   - Nome: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`
   - Versão: se ela permanecer vazia, você receberá a versão mais recente do agente de GuardDuty segurança. Para obter mais informações sobre as versões de lançamento,GuardDuty agente de segurança para instâncias do Amazon EC2.
6. Selecione a instância alvo do Amazon EC2. Você pode selecionar uma ou mais instâncias do Amazon EC2. Para obter mais informações, consulte AWS Systems Manager Executando comandos do console no Guia AWS Systems Manager do usuário
7. Valide se a instalação do GuardDuty agente está íntegra. Para ter mais informações, consulte Validando o status GuardDuty de instalação do agente de segurança.

Método 2 - Usando scripts de instalação do RPM

> **Important**
>
> É altamente recomendável verificar a assinatura RPM do agente de GuardDuty segurança antes de instalá-la em sua máquina.

1. Verifique a assinatura RPM do agente de GuardDuty segurança

   a. Baixe a chave pública apropriada, a assinatura de x86_64 RPM, a assinatura de arm64 RPM e o link de acesso correspondente aos scripts de RPM hospedados nos buckets do Amazon S3

      Você pode usar os modelos a seguir para formar a chave pública, a assinatura de x86_64 RPM, a assinatura de arm64 RPM e o link de acesso correspondente aos scripts de RPM. Substitua o valor do Região da AWS ID da AWS conta e a versão do GuardDuty agente para acessar os scripts de RPM.

- Chave pública:

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/publickey.pem
```

- GuardDuty assinatura RPM do agente de segurança:

  Assinatura de x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/
amazon-guardduty-agent-1.1.0.x86_64.sig
```

  Assinatura do arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/
amazon-guardduty-agent-1.1.0.arm64.sig
```

- Acesse os links para os scripts de RPM no bucket do Amazon S3:

  Link de acesso para x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/
amazon-guardduty-agent-1.1.0.x86_64.rpm
```

  Link de acesso para arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/
amazon-guardduty-agent-1.1.0.arm64.rpm
```

No comando a seguir, para baixar a chave pública apropriada, a assinatura de x86_64 RPM, a assinatura de arm64 RPM e o link de acesso correspondente aos scripts de RPM hospedados nos buckets do Amazon S3, certifique-se de substituir o ID da conta pelo Conta da AWS ID apropriado e a região pela sua região atual.

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/
x86_64/amazon-guardduty-agent-1.1.0.x86_64.rpm ./amazon-guardduty-
agent-1.1.0.x86_64.rpm
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/
x86_64/amazon-guardduty-agent-1.1.0.x86_64.sig ./amazon-guardduty-
agent-1.1.0.x86_64.sig
```

```
aws s3 cp s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/
publickey.pem ./publickey.pem
```

Região da AWS	Nome da região	AWS ID da conta
eu-west-1	Europa (Irlanda)	694911143906
us-east-1	Leste dos EUA (Norte da Virgínia)	593207742271
us-west-2	Oeste dos EUA (Oregon)	733349766148
eu-west-3	Europa (Paris)	665651866788
us-east-2	Leste dos EUA (Ohio)	307168627858
eu-central-1	Europa (Frankfurt)	323658145986
ap-northeast-2	Ásia-Pacífico (Seul)	914738172881
eu-north-1	Europa (Estocolmo)	591436053604
ap-east-1	Ásia-Pacífico (Hong Kong)	258348409381
me-south-1	Oriente Médio (Barém)	536382113932
eu-west-2	Europa (Londres)	892757235363
ap-northeast-1	Ásia-Pacífico (Tóquio)	533107202818
ap-southeast-1	Ásia-Pacífico (Singapura)	174946120834
ap-south-1	Ásia-Pacífico (Mumbai)	251508486986
ap-southeast-3	Ásia-Pacífico (Jacarta)	510637619217
sa-east-1	América do Sul (São Paulo)	758426053663
ap-northeast-3	Asia Pacific (Osaka)	273192626886
eu-south-1	Europa (Milão)	266869475730

af-south-1	África (Cidade do Cabo)	197869348890
ap-southeast-2	Ásia-Pacífico (Sydney)	00:5257.825.471
me-central-1	Oriente Médio (Emirados Árabes Unidos)	00:00:1452.1398
us-west-1	Oeste dos EUA (N. da Califórnia)	684579721401
ca-central-1	Canadá (Central)	354763396469
ap-south-2	Ásia-Pacífico (Hyderabad)	950823858135
eu-south-2	Europa (Espanha)	919611009337
eu-central-2	Europa (Zurique)	529164026651
ap-southeast-4	Ásia-Pacífico (Melbourne)	251357961535
il-central-1	Israel (Tel Aviv)	870907303882

b. Importar a chave pública para o banco de dados

```
gpg --import publickey.pem
```

gpg mostra a importação com sucesso

```
gpg: key 093FF49D: public key "AwsGuardDuty" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

c. Verifique a assinatura

```
gpg --verify amazon-guardduty-agent-1.1.0.x86_64.sig amazon-guardduty-
agent-1.1.0.x86_64.rpm
```

Se a verificação for aprovada, você verá uma mensagem semelhante ao resultado abaixo. Agora você pode prosseguir com a instalação do agente GuardDuty de segurança usando o RPM.

Resultado do exemplo:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: Good signature from "AwsGuardDuty"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 7478 91EF 5378 1334 4456  7603 06C9 06A7 093F F49D
```

Se a verificação falhar, isso significa que a assinatura no RPM foi potencialmente adulterada. Você deve remover a chave pública do banco de dados e repetir o processo de verificação.

Exemplo:

```
gpg: Signature made Fri 17 Nov 2023 07:58:11 PM UTC using ? key ID 093FF49D
gpg: BAD signature from "AwsGuardDuty"
```

d. Remova a chave pública do banco de dados.

```
gpg --delete-keys AwsGuardDuty
```

2. Conecte-se com SSH usando Linux ou macOS.
3. Instale o agente de GuardDuty segurança usando o seguinte comando:

```
sudo rpm -ivh amazon-guardduty-agent-1.1.0.x86_64.rpm
```

4. Valide se a instalação do GuardDuty agente está íntegra. Para obter mais informações sobre as etapas, consulteValidando o status GuardDuty de instalação do agente de segurança.
5. (Opcional) remova o agente de GuardDuty segurança usando o seguinte comando:

```
sudo rpm -ev amazon-guardduty-agent
```

Erro de falta de memória

Se você tiver um `out-of-memory` erro ao instalar ou atualizar manualmente o agente GuardDuty de segurança do Amazon EC2, consulte. Solução de problemas de erro de falta de memória

Validando o status GuardDuty de instalação do agente de segurança

Para validar se o agente de GuardDuty segurança está íntegro

1. Conecte-se com SSH usando Linux ou macOS.
2. Execute o comando a seguir para verificar o status do agente GuardDuty de segurança:

```
sudo systemctl status amazon-guardduty-agent
```

Se você quiser ver os registros de instalação do Security Agent, eles estão disponíveis em`/var/log/amzn-guardduty-agent/`.

Para ver os registros, faça`sudo journalctl -u amazon-guardduty-agent`.

Atualizando o agente GuardDuty de segurança manualmente

Você pode atualizar o agente GuardDuty de segurança usando o comando Executar. Você pode seguir as mesmas etapas usadas para instalar o agente GuardDuty de segurança.

Desinstalando o agente de segurança manualmente

Quando você desativa o Runtime Monitoring, GuardDuty não remove o agente de segurança associado à sua instância do Amazon EC2. Você pode desinstalar o agente GuardDuty de segurança para a instância do Amazon EC2 usando um dos dois métodos a seguir.

Método 1 - Usando o comando Executar

Para desinstalar o agente GuardDuty de segurança usando o comando Executar

1. Você pode desinstalar o agente GuardDuty de segurança seguindo as etapas especificadas em AWS Systems Manager Executar comando no Guia do AWS Systems Manager usuário. Use a ação Desinstalar nos parâmetros para desinstalar o agente GuardDuty de segurança.

   Na seção Metas, certifique-se de que o impacto seja somente nas instâncias do Amazon EC2 das quais você deseja desinstalar o agente de segurança.

   Use o seguinte GuardDuty documento e distribuidor:

   - Nome do documento: `AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin`
   - Distribuidor: `AmazonGuardDuty-RuntimeMonitoringSsmPlugin`

2. Depois de fornecer todos os detalhes, quando você escolhe Executar, o agente de segurança que ele implantou nas instâncias alvo do Amazon EC2 é removido.

   Para remover a configuração do endpoint do Amazon VPC, você deve desativar o Runtime Monitoring e o Amazon EKS Runtime Monitoring.

Método 2 - Usando o script RPM

Para desinstalar o agente GuardDuty de segurança usando o rpm

1. Conecte-se com SSH usando Linux ou macOS.
2. O comando a seguir desinstalará o agente de GuardDuty segurança da instância do Amazon EC2 à qual você se conecta:

   ```
   sudo rpm -e amazon-guardduty-agent
   ```

   Você também pode verificar os registros associados a esse comando.

Excluir o endpoint da Amazon VPC

Quando quiser desativar o Runtime Monitoring ou desinstalar o agente de GuardDuty segurança da sua conta, você também pode optar por excluir o endpoint da Amazon VPC que foi criado manualmente (). Criação manual do endpoint Amazon VPC

Para excluir o endpoint da Amazon VPC usando o console

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, escolha Endpoints.
3. Selecione o endpoint que foi criado manualmente no momento da ativação do Runtime Monitoring.
4. Escolha Actions (Ações), Delete VPC endpoints (Excluir endpoints da VPC).
5. Quando a confirmação for solicitada, insira **`delete`**.
6. Escolha Delete.

Para excluir o endpoint da Amazon VPC usando AWS CLI

- delete-vpc-endpoints (AWS Command Line Interface)

- VpcEndpoint Cmdlet Remove-EC2 (Ferramentas para Windows) PowerShell

Gerenciamento de agente de segurança automatizado para Fargate (somente Amazon ECS)

Configurando o GuardDuty agente para uma conta independente

Atualmente, o Runtime Monitoring oferece suporte ao gerenciamento do agente de segurança para seus clusters do Amazon ECS (AWS Fargate) somente por meio de. GuardDuty Não há suporte para gerenciar o agente de segurança manualmente nos clusters do Amazon ECS.

Console

1. Faça login no AWS Management Console e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Runtime Monitoring.
3. Na guia Configuração:

   a. Para gerenciar a configuração automatizada de agentes para todos os clusters do Amazon ECS (nível da conta)

      Escolha Ativar na seção Configuração automatizada do agente para AWS Fargate (somente ECS). Quando uma nova tarefa do Fargate Amazon ECS for iniciada, GuardDuty gerenciará a implantação do agente de segurança.

      - Selecione Salvar.

   b. Para gerenciar a configuração automatizada do agente excluindo alguns dos clusters do Amazon ECS (nível de cluster)

      i. Adicione uma tag ao cluster do Amazon ECS do qual você deseja excluir todas as tarefas. O par de valores-chave deve ser `GuardDutyManaged` -. `false`

      ii. Evite a modificação dessas tags, exceto por entidades confiáveis. A política fornecida em Impedir que as etiquetas sejam modificadas, exceto pelos princípios autorizados no Guia AWS Organizations do Usuário, foi modificada para ser aplicável aqui.

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

```
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
```

```
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

iii. Na guia Configuração, escolha Ativar na seção Configuração automatizada do agente.

> **Note**
>
> Sempre adicione a tag de exclusão ao seu cluster do Amazon ECS antes de ativar o gerenciamento automático do GuardDuty agente para sua conta; caso contrário, o agente de segurança será implantado em todas as tarefas que forem iniciadas no cluster correspondente do Amazon ECS.

Para os clusters do Amazon ECS que não foram excluídos, GuardDuty gerenciaremos a implantação do agente de segurança no contêiner auxiliar.

iv. Selecione Salvar.

c. Para gerenciar a configuração automatizada de agentes incluindo alguns dos clusters do Amazon ECS (nível de cluster)

   i. Adicione uma tag a um cluster do Amazon ECS no qual você deseja incluir todas as tarefas. O par de valores-chave deve ser `GuardDutyManaged` -. `true`

   ii. Evite a modificação dessas tags, exceto por entidades confiáveis. A política fornecida em Impedir que as etiquetas sejam modificadas, exceto pelos princípios autorizados no Guia AWS Organizations do Usuário, foi modificada para ser aplicável aqui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
```

```
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged":
 "${aws:PrincipalTag/GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/
org-admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

Configurando o GuardDuty agente para um ambiente com várias contas

Em um ambiente de várias contas, somente a conta de GuardDuty administrador delegado pode ativar ou desativar a configuração automática do agente para as contas dos membros e gerenciar a configuração automática do agente para clusters do Amazon ECS que pertencem às contas membros em sua organização. Uma conta de GuardDuty membro não pode modificar essa configuração. A conta de GuardDuty administrador delegado gerencia suas contas de membros usando AWS Organizations. Para obter mais informações sobre ambientes com várias contas, consulte Gerenciando várias contas em GuardDuty.

Habilitando a configuração automatizada do agente para a conta de GuardDuty administrador delegado

Manage for all Amazon ECS clusters (account level)

Se você escolher Habilitar para todas as contas para o Runtime Monitoring, terá as seguintes opções:

- Escolha Ativar para todas as contas na seção Configuração automática do agente. GuardDuty implantará e gerenciará o agente de segurança para todas as tarefas do Amazon ECS que forem lançadas.
- Escolha Configurar contas manualmente.

Se você escolheu Configurar contas manualmente na seção Runtime Monitoring, faça o seguinte:

1. Escolha Configurar contas manualmente na seção Configuração automática do agente.
2. Escolha Habilitar na seção Conta de GuardDuty administrador delegado (esta conta).

Selecione Salvar.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Adicione uma tag a esse cluster do Amazon ECS com o par de valores-chave como -. `GuardDutyManaged false`
2. Impeça a modificação de tags, exceto pelas entidades confiáveis. A política fornecida em Impedir que as etiquetas sejam modificadas, exceto pelos princípios autorizados no Guia AWS Organizations do Usuário, foi modificada para ser aplicável aqui.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
```

```
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
4. No painel de navegação, escolha Runtime Monitoring.
5.

> **Note**
>
> Sempre adicione a tag de exclusão aos seus clusters do Amazon ECS antes de ativar a configuração automática do agente para sua conta; caso contrário, o contêiner GuardDuty auxiliar será anexado a todos os contêineres nas tarefas do Amazon ECS que forem iniciadas.

Na guia Configuração, escolha Ativar na configuração automatizada do agente.

Para os clusters do Amazon ECS que não foram excluídos, GuardDuty gerenciaremos a implantação do agente de segurança no contêiner auxiliar.

6. Selecione Salvar.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Adicione uma tag a um cluster do Amazon ECS no qual você deseja incluir todas as tarefas. O par de valores-chave deve ser `GuardDutyManaged` -. `true`
2. Evite a modificação dessas tags, exceto por entidades confiáveis. A política fornecida em Impedir que as etiquetas sejam modificadas, exceto pelos princípios autorizados no Guia AWS Organizations do Usuário, foi modificada para ser aplicável aqui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
```

```
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Ao usar tags de inclusão para seus clusters do Amazon ECS, você não precisa habilitar explicitamente o GuardDuty agente por meio da configuração automática do agente.

Ativação automática para todas as contas de membros

Manage for all Amazon ECS clusters (account level)

As etapas a seguir pressupõem que você escolheu Habilitar para todas as contas na seção Monitoramento de tempo de execução.

1. Escolha Ativar para todas as contas na seção Configuração automática do agente. GuardDuty implantará e gerenciará o agente de segurança para todas as tarefas do Amazon ECS que forem lançadas.
2. Selecione Salvar.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Adicione uma tag a esse cluster do Amazon ECS com o par de valores-chave como -. `GuardDutyManaged` `false`
2. Impeça a modificação de tags, exceto pelas entidades confiáveis. A política fornecida em Impedir que as etiquetas sejam modificadas, exceto pelos princípios autorizados no Guia AWS Organizations do Usuário, foi modificada para ser aplicável aqui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
```

```
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
```

```
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
4. No painel de navegação, escolha Runtime Monitoring.
5.

> **Note**
>
> Sempre adicione a tag de exclusão aos seus clusters do Amazon ECS antes de ativar a configuração automática do agente para sua conta; caso contrário, o contêiner GuardDuty auxiliar será anexado a todos os contêineres nas tarefas do Amazon ECS que forem iniciadas.

   Na guia Configuração, escolha Editar.
6. Escolha Ativar para todas as contas na seção Configuração automática do agente

   Para os clusters do Amazon ECS que não foram excluídos, GuardDuty gerenciaremos a implantação do agente de segurança no contêiner auxiliar.
7. Selecione Salvar.

Manage for selective (inclusion-only) Amazon ECS clusters (cluster level)

Independentemente de como você optar por ativar o Runtime Monitoring, as etapas a seguir ajudarão você a monitorar tarefas seletivas do Amazon ECS Fargate para todas as contas membros da sua organização.

1. Não habilite nenhuma configuração na seção Configuração automatizada do agente. Mantenha a configuração do Runtime Monitoring igual à selecionada na etapa anterior.
2. Selecione Salvar.
3. Evite a modificação dessas tags, exceto por entidades confiáveis. A política fornecida em Impedir que as etiquetas sejam modificadas, exceto pelos princípios autorizados no Guia AWS Organizations do Usuário, foi modificada para ser aplicável aqui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
```

```
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Ao usar tags de inclusão para seus clusters do Amazon ECS, você não precisa habilitar explicitamente o gerenciamento automático de GuardDuty agentes.

Habilitando a configuração automatizada de agentes para contas de membros ativos existentes

Manage for all Amazon ECS clusters (account level)

1. Na página Runtime Monitoring, na guia Configuração, você pode ver o status atual da configuração automatizada do agente.
2. No painel Configuração automatizada do agente, na seção Contas de membros ativas, escolha Ações.
3. Em Ações, escolha Habilitar para todas as contas-membro ativas existentes.
4. Selecione a opção Confirmar.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Adicione uma tag a esse cluster do Amazon ECS com o par de valores-chave como -. `GuardDutyManaged` `false`
2. Impeça a modificação de tags, exceto pelas entidades confiáveis. A política fornecida em Impedir que as etiquetas sejam modificadas, exceto pelos princípios autorizados no Guia AWS Organizations do Usuário, foi modificada para ser aplicável aqui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
```

```
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
```

```
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
4. No painel de navegação, escolha Runtime Monitoring.
5.

> **Note**
>
> Sempre adicione a tag de exclusão aos seus clusters do Amazon ECS antes de ativar a configuração automática do agente para sua conta; caso contrário, o contêiner GuardDuty auxiliar será anexado a todos os contêineres nas tarefas do Amazon ECS que forem iniciadas.

   Na guia Configuração, na seção Configuração automatizada do agente, em Contas de membros ativas, escolha Ações.
6. Em Ações, escolha Habilitar para todas as contas-membro ativas.

   Para os clusters do Amazon ECS que não foram excluídos, GuardDuty gerenciaremos a implantação do agente de segurança no contêiner auxiliar.
7. Selecione a opção Confirmar.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Adicione uma tag a um cluster do Amazon ECS no qual você deseja incluir todas as tarefas. O par de valores-chave deve ser `GuardDutyManaged` -. `true`
2. Evite a modificação dessas tags, exceto por entidades confiáveis. A política fornecida em Impedir que as etiquetas sejam modificadas, exceto pelos princípios autorizados no Guia AWS Organizations do Usuário, foi modificada para ser aplicável aqui.

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

```
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
```

```
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Ao usar tags de inclusão para seus clusters do Amazon ECS, você não precisa habilitar explicitamente a configuração automatizada do agente.

Ativar automaticamente a configuração automatizada do agente para novos membros

Manage for all Amazon ECS clusters (account level)

1. Na página Runtime Monitoring, escolha Editar para atualizar a configuração existente.
2. Na seção Configuração automatizada do agente, selecione Ativar automaticamente para novas contas de membros.
3. Selecione Salvar.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Adicione uma tag a esse cluster do Amazon ECS com o par de valores-chave como -. `GuardDutyManaged` `false`
2. Impeça a modificação de tags, exceto pelas entidades confiáveis. A política fornecida em Impedir que as etiquetas sejam modificadas, exceto pelos princípios autorizados no Guia AWS Organizations do Usuário, foi modificada para ser aplicável aqui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
```

```
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
4. No painel de navegação, escolha Runtime Monitoring.

5.

> **Note**
>
> Sempre adicione a tag de exclusão aos seus clusters do Amazon ECS antes de ativar a configuração automática do agente para sua conta; caso contrário, o contêiner GuardDuty auxiliar será anexado a todos os contêineres nas tarefas do Amazon ECS que forem iniciadas.

   Na guia Configuração, selecione Ativar automaticamente para novas contas de membros na seção Configuração automatizada do agente.

   Para os clusters do Amazon ECS que não foram excluídos, GuardDuty gerenciaremos a implantação do agente de segurança no contêiner auxiliar.

6. Selecione Salvar.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Adicione uma tag a um cluster do Amazon ECS no qual você deseja incluir todas as tarefas. O par de valores-chave deve ser `GuardDutyManaged` -. `true`
2. Evite a modificação dessas tags, exceto por entidades confiáveis. A política fornecida em Impedir que as etiquetas sejam modificadas, exceto pelos princípios autorizados no Guia AWS Organizations do Usuário, foi modificada para ser aplicável aqui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
```

```
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Ao usar tags de inclusão para seus clusters do Amazon ECS, você não precisa habilitar explicitamente a configuração automatizada do agente.

Habilitando a configuração automatizada de agentes para contas de membros ativos de forma seletiva

Manage for all Amazon ECS (account level)

1. Na página Contas, selecione as contas para as quais você deseja ativar a configuração automática do agente Runtime Monitoring-Automated (ECS-Fargate). Você pode selecionar várias contas. Certifique-se de que as contas selecionadas nesta etapa já estejam habilitadas com o Runtime Monitoring.
2. Em Editar planos de proteção, escolha a opção apropriada para ativar a configuração automática do agente Runtime Monitoring-Automated (ECS-Fargate).
3. Selecione a opção Confirmar.

Manage for all Amazon ECS clusters but exclude some of the clusters (cluster level)

1. Adicione uma tag a esse cluster do Amazon ECS com o par de valores-chave como -. `GuardDutyManaged` `false`

2. Impeça a modificação de tags, exceto pelas entidades confiáveis. A política fornecida em Impedir que as etiquetas sejam modificadas, exceto pelos princípios autorizados no Guia AWS Organizations do Usuário, foi modificada para ser aplicável aqui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
4. No painel de navegação, escolha Runtime Monitoring.
5.

> **Note**
>
> Sempre adicione a tag de exclusão aos seus clusters do Amazon ECS antes de ativar o gerenciamento automático do GuardDuty agente para sua conta; caso contrário, o GuardDuty contêiner auxiliar será anexado a todos os contêineres nas tarefas do Amazon ECS que forem iniciadas.

Na página Contas, selecione as contas para as quais você deseja ativar a configuração automática do agente Runtime Monitoring-Automated (ECS-Fargate). Você pode selecionar várias contas. Certifique-se de que as contas selecionadas nesta etapa já estejam habilitadas com o Runtime Monitoring.

Para os clusters do Amazon ECS que não foram excluídos, GuardDuty gerenciaremos a implantação do agente de segurança no contêiner auxiliar.

6. Em Editar planos de proteção, escolha a opção apropriada para ativar a configuração automática do agente Runtime Monitoring-Automated (ECS-Fargate).
7. Selecione Salvar.

Manage for selective (inclusion only) Amazon ECS clusters (cluster level)

1. Certifique-se de não habilitar a configuração automática do agente (ou Runtime Monitoring-Automated Agent Configuration (ECS-Fargate)) para as contas selecionadas que têm os clusters do Amazon ECS que você deseja monitorar.
2. Adicione uma tag a um cluster do Amazon ECS no qual você deseja incluir todas as tarefas. O par de valores-chave deve ser `GuardDutyManaged` -. `true`
3. Evite a modificação dessas tags, exceto por entidades confiáveis. A política fornecida em Impedir que as etiquetas sejam modificadas, exceto pelos princípios autorizados no Guia AWS Organizations do Usuário, foi modificada para ser aplicável aqui.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "ecs:ResourceTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "ecs:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/GuardDutyManaged": "${aws:PrincipalTag/
GuardDutyManaged}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ecs:CreateTags",
                "ecs:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
```

```
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-
admins/iam-admin"
                },
                "Null": {
                    "aws:PrincipalTag/GuardDutyManaged": true
                }
            }
        }
    ]
}
```

> **Note**
>
> Ao usar tags de inclusão para seus clusters do Amazon ECS, você não precisa habilitar explicitamente a configuração automatizada do agente.

Gerenciando automaticamente o agente de segurança para clusters do Amazon EKS

Configurando o agente automatizado para uma conta independente

1. Faça login no AWS Management Console e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Runtime Monitoring.
3. Na guia Configuração, escolha Ativar para ativar a configuração automática do agente para sua conta.

Abordagem preferida para implantar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (Monitorar todos os clusters do EKS)	1. Escolha Ativar na seção Configuração automatizada do agente. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters EKS existentes e potencialmente novos em sua conta.

Abordagem preferida para implantar o agente GuardDuty de segurança	Etapas
	2. Selecione Salvar.

Abordagem preferida para implantar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando a tag de exclusão)	Nos procedimentos a seguir, escolha um dos cenários que se aplica a você. Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança não foi implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2: CreateTags`* por `eks:TagResource` . • Substitua *`ec2: DeleteTags`* por `eks:UntagResource` . • Substitua *`access-project`* por `GuardDutyManaged` • Substitua *`123456789012`* pela ID da Conta da AWS entidade confiável.

Abordagem preferida para implantar o agente GuardDuty de segurança	Etapas
	Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/. 4. No painel de navegação, escolha Runtime Monitoring. **Note** Sempre adicione a tag de exclusão aos seus clusters EKS antes de ativar o gerenciamento automático de GuardDuty agentes para sua conta; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta. 5. Na guia Configuração, escolha Habilitar na seção Gerenciamento de GuardDuty agentes. Para os clusters EKS que não foram excluídos do monitoramento, GuardDuty gerenciará a implantação e as atualizações do agente GuardDuty de segurança. 6. Selecione Salvar.

Abordagem preferida para implantar o agente GuardDuty de segurança	Etapas
	Para excluir um cluster EKS do monitoramento após o agente GuardDuty de segurança já ter sido implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. Após essa etapa, não GuardDuty atualizará o agente de segurança desse cluster. No entanto, o agente de segurança permanecerá implantado e GuardDuty continuará recebendo os eventos de tempo de execução desse cluster EKS. Isso pode afetar as estatísticas sobre seu uso. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged`

Abordagem preferida para implantar o agente GuardDuty de segurança	Etapas
	• Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Para parar de receber os eventos de runtime desse cluster, você deve remover o agente de segurança implantado desse cluster do EKS. Para obter mais informações sobre a remoção do agente de segurança implantado, consulte Limpando os recursos do agente de GuardDuty segurança.

Abordagem preferida para implantar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos usando tags de inclusão	1. Certifique-se de escolher Desativar na seção Configuração automática do agente. Mantenha o Runtime Monitoring ativado. 2. Escolha Salvar 3. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `true`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. GuardDuty gerenciará a implantação e as atualizaç ões do agente de segurança para os clusters EKS seletivos que você deseja monitorar. 4. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2: CreateTags`* `poreks:TagResource` . • Substitua *`ec2: DeleteTags`* `poreks:UntagResource` . • Substitua *`access-project`* por `GuardDutyManaged` • Substitua *`123456789012`* pela ID da Conta da AWS entidade confiável.

Abordagem preferida para implantar o agente GuardDuty de segurança	Etapas
	Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Gerenciar agente manualmente	1. Certifique-se de escolher Desativar na seção Configuração automática do agente. Mantenha o Runtime Monitoring ativado. 2. Escolha Salvar. 3. Para gerenciar o agente de segurança, consulte Gerenciando o agente de segurança manualmente para o cluster Amazon EKS.

Configurando o agente automatizado para ambientes com várias contas

Em ambientes de várias contas, somente a conta de GuardDuty administrador delegado pode ativar ou desativar a configuração automatizada do agente para as contas dos membros e gerenciar o agente automatizado para os clusters EKS pertencentes às contas dos membros em sua organização. As contas GuardDuty dos membros não podem modificar essa configuração em suas contas. A conta de GuardDuty administrador delegado gerencia suas contas de membros usando AWS Organizations. Para obter mais informações sobre ambientes com várias contas, consulte Gerenciar de várias contas.

Configurando a configuração automatizada do agente para a conta de administrador delegado GuardDuty

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (Monitorar todos os clusters do EKS)	Se você escolher Habilitar para todas as contas na seção Runtime Monitoring, terá as seguintes opções: • Escolha Ativar para todas as contas na seção Configuração automática do agente. GuardDuty implantará e gerenciará o agente de segurança para todos os clusters EKS que pertencem à conta de GuardDuty administrador delegada e também para todos os clusters EKS que pertencem a todas as contas membros existentes e potencialmente novas na organização. • Escolha Configurar contas manualmente. Se você escolheu Configurar contas manualmente na seção Runtime Monitoring, faça o seguinte: 1. Escolha Configurar contas manualmente na seção Configuração automática do agente. 2. Escolha Habilitar na seção Conta de GuardDuty administrador delegado (esta conta). Escolha Salvar.
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando tags de exclusão)	Nos procedimentos a seguir, escolha um dos cenários aplicáveis a você. Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança não foi implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas

Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS.

2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes:

   - Substitua *ec2: CreateTags* por `eks:TagResource` .
   - Substitua *ec2: DeleteTags* por `eks:UntagResource` .
   - Substitua *access-project* por `GuardDutyManaged`
   - Substitua *123456789012* pela ID da Conta da AWS entidade confiável.

     Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` :

     ```
     "aws:PrincipalArn":["arn:aws:iam::12345678901
     2:role/org-admins/iam-admin", "arn:aws:iam::1234
     56789012:role/org-admins/iam-admin", "arn:aws:
     iam::123456789012:role/org-admins/iam-admin"]
     ```

3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
4. No painel de navegação, escolha Runtime Monitoring.

   > **Note**
   >
   > Sempre adicione a tag de exclusão aos seus clusters EKS antes de ativar o gerenciamento automático de GuardDuty agentes para sua conta; caso contrário, o

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta. 5. Na guia Configuração, escolha Habilitar na seção Gerenciam ento de GuardDuty agentes. Para os clusters EKS que não foram excluídos do monitoram ento, GuardDuty gerenciará a implantação e as atualizações do agente GuardDuty de segurança. 6. Selecione Salvar. Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança foi implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Se você tiver habilitado o agente automatizado para esse cluster EKS, depois dessa etapa, não GuardDuty atualizará o agente de segurança desse cluster. No entanto, o agente de segurança permanecerá implantado e GuardDuty continuará recebendo os eventos de tempo de execução desse cluster EKS. Isso pode afetar as estatísticas sobre seu uso. Para parar de receber os eventos de runtime desse cluster, você deve remover o agente de segurança implantado desse cluster do EKS. Para obter mais informações sobre a remoção do agente de segurança implantado, consulte Limpando os recursos do agente de GuardDuty segurança 4. Se você estava gerenciando o agente de GuardDuty segurança desse cluster EKS manualmente, consulteLimpando os recursos do agente de GuardDuty segurança.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos usando tags de inclusão	Independentemente de como você escolheu ativar o Runtime Monitoring, as etapas a seguir ajudarão você a monitorar clusters EKS seletivos em sua conta: 1. Certifique-se de escolher Desativar para conta de GuardDuty administrador delegado (esta conta) na seção Configuração automatizada do agente. Mantenha a configuração do Runtime Monitoring igual à configurada na etapa anterior. 2. Escolha Salvar. 3. Adicione uma tag ao seu cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `true`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para os clusters EKS seletivos que você deseja monitorar. 4. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` :

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	`"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Gerencie o agente GuardDuty de segurança manualmente	Independentemente de como você escolheu ativar o Runtime Monitoring, você pode gerenciar o agente de segurança manualmente para seus clusters EKS. 1. Certifique-se de escolher Desativar para conta de GuardDuty administrador delegado (esta conta) na seção Configuração automatizada do agente. Mantenha a configuração do Runtime Monitoring igual à configurada na etapa anterior. 2. Escolha Salvar. 3. Para gerenciar o agente de segurança, consulte Gerenciando o agente de segurança manualmente para o cluster Amazon EKS.

Ativar automaticamente o agente automatizado para todas as contas dos membros

> **Note**
>
> Pode levar até 24 horas para atualizar a configuração das contas-membro.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty	Este tópico é para ativar o Monitoramento de Tempo de Execução para todas as contas de membros e, portanto, as etapas a seguir pressupõem que você tenha escolhido Habilitar para todas as contas na seção Monitoramento de Tempo de Execução.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
(Monitorar todos os clusters do EKS)	1. Escolha Ativar para todas as contas na seção Configuração automática do agente. GuardDuty implantará e gerenciará o agente de segurança para todos os clusters EKS que pertencem à conta de GuardDuty administrador delegada e também para todos os clusters EKS que pertencem a todas as contas membros existentes e potencialmente novas na organização. 2. Escolha Salvar.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando tags de exclusão)	Nos procedimentos a seguir, escolha um dos cenários aplicáveis a você. Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança não foi implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2: CreateTags`* por `eks:TagResource` . • Substitua *`ec2: DeleteTags`* por `eks:UntagResource` . • Substitua *`access-project`* por `GuardDutyManaged` • Substitua *`123456789012`* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	4. No painel de navegação, escolha Runtime Monitoring. **Note** Sempre adicione a tag de exclusão aos seus clusters EKS antes de ativar o agente automatizado para sua conta; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta. 5. Na guia Configuração, escolha Editar na seção Configuração do Runtime Monitoring. 6. Escolha Ativar para todas as contas na seção Configuração automática do agente. Para os clusters EKS que não foram excluídos do monitoramento, GuardDuty gerenciará a implantaç ão e as atualizações do agente GuardDuty de segurança. 7. Selecione Salvar. Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança foi implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. 2. Se você tiver a configuração automatizada do agente habilitad a para esse cluster EKS, depois dessa etapa, não GuardDuty atualizará o agente de segurança desse cluster. No entanto, o agente de segurança permanecerá implantado e GuardDuty continuará recebendo os eventos de tempo de execução desse cluster EKS. Isso pode afetar as estatísticas sobre seu uso.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Para parar de receber os eventos de runtime desse cluster, você deve remover o agente de segurança implantado desse cluster do EKS. Para obter mais informações sobre a remoção do agente de segurança implantado, consulte Limpando os recursos do agente de GuardDuty segurança 3. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 4. Se você estava gerenciando o agente de GuardDuty segurança desse cluster EKS manualmente, consulteLimpando os recursos do agente de GuardDuty segurança.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos usando tags de inclusão	Independentemente de como você escolheu ativar o Runtime Monitoring, as etapas a seguir ajudarão você a monitorar clusters EKS seletivos para todas as contas membros em sua organização: 1. Não habilite nenhuma configuração na seção Configuração automatizada do agente. Mantenha a configuração do Runtime Monitoring igual à configurada na etapa anterior. 2. Escolha Salvar. 3. Adicione uma tag ao seu cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `true`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para os clusters EKS seletivos que você deseja monitorar. 4. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2: CreateTags`* por `eks:TagResource` . • Substitua *`ec2: DeleteTags`* por `eks:UntagResource` . • Substitua *`access-project`* por `GuardDutyManaged` • Substitua *`123456789012`* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` :

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	`"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Gerencie o agente GuardDuty de segurança manualmente	Independentemente de como você escolheu ativar o Runtime Monitoring, você pode gerenciar o agente de segurança manualmente para seus clusters EKS. 1. Não habilite nenhuma configuração na seção Configuração automatizada do agente. Mantenha a configuração do Runtime Monitoring igual à configurada na etapa anterior. 2. Escolha Salvar. 3. Para gerenciar o agente de segurança, consulte Gerenciando o agente de segurança manualmente para o cluster Amazon EKS.

Habilitando o agente automatizado para todas as contas de membros ativos existentes

> **Note**
>
> Pode levar até 24 horas para atualizar a configuração das contas-membro.

Para gerenciar o agente GuardDuty de segurança para contas de membros ativos existentes em sua organização

- GuardDuty Para receber os eventos de tempo de execução dos clusters EKS que pertencem às contas de membros ativos existentes na organização, você deve escolher uma abordagem preferida para gerenciar o agente de GuardDuty segurança desses clusters EKS. Para obter mais informações sobre essas abordagens, consulte Abordagens para gerenciar o agente GuardDuty de segurança.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (Monitorar todos os clusters do EKS)	Para monitorar todos os clusters do EKS para todas as contas-membro ativas existentes 1. Na página Runtime Monitoring, na guia Configuração, você pode ver o status atual da configuração automatizada do agente. 2. No painel Configuração automatizada do agente, na seção Contas de membros ativas, escolha Ações. 3. Em Ações, escolha Habilitar para todas as contas-membro ativas existentes. 4. Selecione a opção Confirmar.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando a tag de exclusão)	Nos procedimentos a seguir, escolha um dos cenários aplicáveis a você. Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança não foi implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/. 4. No painel de navegação, escolha Runtime Monitoring. **Note** Sempre adicione a tag de exclusão aos seus clusters EKS antes de ativar a configuração automática do agente para sua conta; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta. 5. Na guia Configuração, no painel Configuração automatizada do agente, em Contas de membros ativas, escolha Ações. 6. Em Ações, escolha Habilitar para todas as contas-membro ativas. 7. Selecione a opção Confirmar.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Para excluir um cluster EKS do monitoramento após o agente GuardDuty de segurança já ter sido implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. Após essa etapa, não GuardDuty atualizará o agente de segurança desse cluster. No entanto, o agente de segurança permanecerá implantado e GuardDuty continuará recebendo os eventos de tempo de execução desse cluster EKS. Isso pode afetar as estatísticas sobre seu uso. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	• Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Independentemente de como você gerencia o agente de segurança (por meio GuardDuty ou manualmente), para parar de receber os eventos de tempo de execução desse cluster, você deve remover o agente de segurança implantado desse cluster EKS. Para obter mais informações sobre a remoção do agente de segurança implantado, consulte Limpando os recursos do agente de GuardDuty segurança.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos usando tags de inclusão	1. Na página Contas, depois de ativar o Runtime Monitoring, não ative o Runtime Monitoring - Configuração automatizada do agente. 2. Adicione uma tag ao cluster do EKS que pertence à conta selecionada que você deseja monitorar. O par de chave-valor da tag deve ser `GuardDuty Managed -true`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. GuardDuty gerenciará a implantação e as atualizaç ões do agente de segurança para os clusters EKS seletivos que você deseja monitorar. 3. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2: CreateTags`* `poreks:TagRe source` . • Substitua *`ec2: DeleteTags`* `poreks:Untag Resource` . • Substitua *`access-project`* por `GuardDuty Managed` • Substitua *`123456789012`* pela ID da Conta da AWS entidade confiável.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Gerencie o agente GuardDuty de segurança manualmente	1. Certifique-se de não escolher Ativar na seção Configuração automatizada do agente. Mantenha o Runtime Monitoring ativado. 2. Escolha Salvar. 3. Para gerenciar o agente de segurança, consulte Gerenciando o agente de segurança manualmente para o cluster Amazon EKS.

Ative automaticamente a configuração automatizada do agente para novos membros

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (Monitorar todos os clusters do EKS)	1. Na página Runtime Monitoring, escolha Editar para atualizar a configuração existente. 2. Na seção Configuração automatizada do agente, selecione Ativar automaticamente para novas contas de membros. 3. Escolha Salvar.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando tags de exclusão)	Nos procedimentos a seguir, escolha um dos cenários aplicáveis a você. Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança não foi implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` :

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas

```
"aws:PrincipalArn":["arn:aws:iam::12
3456789012:role/org-admins/iam-admin
", "arn:aws:iam::123456789012:role/org-
admins/iam-admin", "arn:aws:iam::1234
56789012:role/org-admins/iam-admin"]
```

3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
4. No painel de navegação, escolha Runtime Monitoring.

> **Note**
>
> Sempre adicione a tag de exclusão aos seus clusters EKS antes de ativar a configuração automática do agente para sua conta; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta.

5. Na guia Configuração, selecione Ativar automatic amente para novas contas de membros na seção de gerenciamento de GuardDuty agentes.

   Para os clusters EKS que não foram excluídos do monitoramento, GuardDuty gerenciará a implantação e as atualizações do agente GuardDuty de segurança.
6. Selecione Salvar.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança foi implantado nesse cluster 1. Independentemente de você gerenciar o agente GuardDuty de segurança por meio GuardDuty ou manualmente, adicione uma tag a esse cluster EKS com a chave como `GuardDutyManaged` e seu valor como`false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. Se você tiver ativado o agente automatizado para esse cluster EKS, depois dessa etapa, não GuardDuty atualizará o agente de segurança desse cluster. No entanto, o agente de segurança permanecerá implantado e GuardDuty continuará recebendo os eventos de tempo de execução desse cluster EKS. Isso pode afetar as estatísticas sobre seu uso. Para parar de receber os eventos de runtime desse cluster, você deve remover o agente de segurança implantado desse cluster do EKS. Para obter mais informações sobre a remoção do agente de segurança implantado, consulte Limpando os recursos do agente de GuardDuty segurança 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes:

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	• Substitua *ec2: CreateTags* por `poreks:TagResource` . • Substitua *ec2: DeleteTags* por `poreks:UntagResource` . • Substitua *access-project* por `GuardDuty Managed` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Se você estava gerenciando o agente de GuardDuty segurança desse cluster EKS manualmente, consulteLimpando os recursos do agente de GuardDuty segurança.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos usando tags de inclusão	Independentemente de como você escolheu ativar o Runtime Monitoring, as etapas a seguir ajudarão você a monitorar clusters EKS seletivos para as novas contas membros em sua organização. 1. Certifique-se de desmarcar a opção Ativar automatic amente para novas contas de membros na seção Configuração automática do agente. Mantenha a configuração do Runtime Monitoring igual à configurada na etapa anterior. 2. Escolha Salvar. 3. Adicione uma tag ao seu cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `true`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para os clusters EKS seletivos que você deseja monitorar. 4. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` .

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	• Substitua *access-project* por `GuardDuty Managed` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Gerencie o agente GuardDuty de segurança manualmente	Independentemente de como você escolheu ativar o Runtime Monitoring, você pode gerenciar o agente de segurança manualmente para seus clusters EKS. 1. Certifique-se de desmarcar a caixa de seleção Ativar automaticamente para novas contas de membros na seção Configuração automática do agente. Mantenha a configuração do Runtime Monitoring igual à configurada na etapa anterior. 2. Escolha Salvar. 3. Para gerenciar o agente de segurança, consulte Gerenciando o agente de segurança manualmente para o cluster Amazon EKS.

Configurando o agente automatizado para contas de membros ativos de forma seletiva

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (Monitorar todos os clusters do EKS)	1. Na página Contas, selecione as contas para as quais você deseja ativar a configuração automatizada do agente. É possível selecionar mais de uma conta por vez. Certifique-se de que as contas selecionadas nesta etapa já tenham o Monitoramento de runtime do EKS habilitado. 2. Em Editar planos de proteção, escolha a opção apropriada para ativar o Runtime Monitoring - Configuração automatizada do agente. 3. Selecione a opção Confirmar.
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando tags de exclusão)	Nos procedimentos a seguir, escolha um dos cenários aplicáveis a você. Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança não foi implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas

- Substitua *123456789012* pela ID da Conta da AWS entidade confiável.

  Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` :

```
"aws:PrincipalArn":["arn:aws:iam::12345678901
2:role/org-admins/iam-admin", "arn:aws:iam::1234
56789012:role/org-admins/iam-admin", "arn:aws:
iam::123456789012:role/org-admins/iam-admin"]
```

3. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   > **Note**
   >
   > Sempre adicione a tag de exclusão aos seus clusters EKS antes de ativar a configuração automática do agente para sua conta; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta.

4. Na página Contas, selecione a conta para a qual você deseja habilitar a opção Gerenciar o agente automaticamente. É possível selecionar mais de uma conta por vez.
5. Em Editar planos de proteção, escolha a opção apropriada para ativar a configuração automática do agente Runtime Monitoring-Automated para a conta selecionada.

   Para os clusters EKS que não foram excluídos do monitoram ento, GuardDuty gerenciará a implantação e as atualizações do agente GuardDuty de segurança.
6. Selecione Salvar.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Para excluir um cluster EKS do monitoramento quando o agente de GuardDuty segurança foi implantado nesse cluster 1. Adicione uma tag a esse cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `false`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. Se você já tinha a configuração automatizada do agente habilitada para esse cluster EKS, depois dessa etapa, não GuardDuty atualizará o agente de segurança desse cluster. No entanto, o agente de segurança permanecerá implantado e GuardDuty continuará recebendo os eventos de tempo de execução desse cluster EKS. Isso pode afetar as estatísticas sobre seu uso. Para parar de receber os eventos de runtime desse cluster, você deve remover o agente de segurança implantado desse cluster do EKS. Para obter mais informações sobre a remoção do agente de segurança implantado, consulte Limpando os recursos do agente de GuardDuty segurança 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Se você estava gerenciando o agente de GuardDuty segurança desse cluster EKS manualmente, você deve removê-lo. Para ter mais informações, consulte Limpando os recursos do agente de GuardDuty segurança.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos usando tags de inclusão	Independentemente de como você escolheu ativar o Runtime Monitoring, as etapas a seguir ajudarão você a monitorar clusters EKS seletivos que pertencem às contas selecionadas: 1. Certifique-se de não habilitar a configuração do agente Runtime Monitoring-Automated para as contas selecionadas que têm os clusters EKS que você deseja monitorar. 2. Adicione uma tag ao seu cluster do EKS com a chave como `GuardDutyManaged` e seu valor como `true`. Para obter mais informações sobre como marcar seu cluster do Amazon EKS, consulte Como trabalhar com tags usando o console no Guia do usuário do Amazon EKS. Depois de adicionar a tag, GuardDuty gerenciará a implantação e as atualizações do agente de segurança para os clusters EKS seletivos que você deseja monitorar. 3. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` :

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	`"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`
Gerencie o agente GuardDuty de segurança manualmente	1. Mantenha a configuração do Runtime Monitoring igual à configurada na etapa anterior. Certifique-se de não ativar o Runtime Monitoring - Configuração automatizada do agente para nenhuma das contas selecionadas. 2. Selecione a opção Confirmar. 3. Para gerenciar o agente de segurança, consulte Gerenciando o agente de segurança manualmente para o cluster Amazon EKS.

Gerenciando o agente de segurança manualmente para o cluster Amazon EKS

Esta seção descreve como você pode gerenciar seu agente complementar (GuardDuty agente) do Amazon EKS depois de ativar o Runtime Monitoring. Para usar o Runtime Monitoring, você deve habilitar o Runtime Monitoring e configurar o complemento Amazon EKS,`aws-guardduty-agent`. Executar apenas uma dessas duas etapas não ajudará a GuardDuty detectar possíveis ameaças ou gerar descobertas.

Pré-requisitos para implantar o agente de segurança GuardDuty

Esta seção descreve os pré-requisitos para implantar manualmente o agente de GuardDuty segurança em seus clusters EKS. Antes de continuar, verifique se você já configurou o Runtime Monitoring para suas contas. O agente GuardDuty de segurança (complemento EKS) não funcionará se você não configurar o Runtime Monitoring. Para ter mais informações, consulte Habilitando o GuardDuty monitoramento de tempo. Depois de concluir as etapas a seguir, consulte Implantando o agente GuardDuty de segurança.

Escolha seu método de acesso preferido para criar um endpoint da Amazon VPC.

Console

Criar endpoint da VPC

1. Abra o console da Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No menu à de navegação, em Nuvem privada virtual, escolha Endpoints.
3. Escolha Criar endpoint.
4. Na página Criar endpoint, para a Categoria de serviço, escolha Outros serviços de endpoint.
5. Em Nome do serviço, digite **com.amazonaws.*us-east-1*.guardduty-data**.

   Substitua *us-east-1* pela região correta. Essa deve ser a mesma região do cluster EKS que pertence ao seu Conta da AWS ID.
6. Selecione Verificar serviço.
7. Depois que o nome do serviço for verificado com sucesso, escolha a VPC em que reside o cluster. Adicione a política a seguir para restringir o uso do endpoint da VPC somente à conta especificada. Com a `Condition` da organização fornecida abaixo desta política, você pode atualizar a política a seguir para restringir o acesso ao seu endpoint. Para fornecer suporte de endpoint da VPC para IDs de conta específicos em sua organização, consulte Organization condition to restrict access to your endpoint.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Action": "*",
   "Resource": "*",
   "Effect": "Allow",
   "Principal": "*"
  },
  {
   "Condition": {
    "StringNotEquals": {
     "aws:PrincipalAccount": "111122223333"
    }
   },
   "Action": "*",
   "Resource": "*",
   "Effect": "Deny",
   "Principal": "*"
  }
```

```
 ]
}
```

O ID de conta `aws:PrincipalAccount` deve corresponder à conta que contém a VPC e o endpoint da VPC. A lista a seguir mostra como compartilhar o endpoint da VPC com outros IDs de Conta da AWS :

Condição da organização para restringir o acesso ao endpoint

- Para especificar várias contas para acessar o endpoint da VPC, substitua `"aws:PrincipalAccount": "111122223333"` pelo seguinte:

```
"aws:PrincipalAccount": [
          "666666666666",
          "555555555555"
    ]
```

- Para permitir que todos os membros de uma organização acessem o endpoint da VPC, substitua `"aws:PrincipalAccount": "111122223333"` pelo seguinte:

```
"aws:PrincipalOrgID": "o-abcdef0123"
```

- Para restringir o acesso para um recurso a um ID de organização, adicione seu `ResourceOrgID` à política.

  Para obter mais informações, consulte ResourceOrgID.

```
"aws:ResourceOrgID": "o-abcdef0123"
```

8. Em Configurações adicionais, selecione Habilitar nome DNS.
9. Em Sub-redes, escolha as sub-redes em que reside seu cluster.
10. Em Grupos de segurança, escolha um grupo de segurança que tenha a porta de entrada 443 habilitada em sua VPC (ou em seu cluster do EKS). Crie um grupo de segurança se ainda não tiver um com uma porta de entrada 443 habilitada.

    Se houver algum problema ao restringir as permissões de entrada para sua VPC (ou cluster), forneça suporte à porta 443 de entrada de qualquer endereço IP (`0.0.0.0/0`).

API/CLI

- Invocar. CreateVpcEndpoint
- Use os valores a seguir para os parâmetros.
  - Em Nome do serviço, digite **`com.amazonaws.`*`us-east-1`*`.guardduty-data`**.

    Substitua *`us-east-1`* pela região correta. Essa deve ser a mesma região do cluster EKS que pertence ao seu Conta da AWS ID.
  - Para DNSOptions, habilite a opção de DNS privado definindo-a como `true`.
- Para AWS Command Line Interface, veja create-vpc-endpoint.

Configurar parâmetros do agente de GuardDuty segurança (complemento) para o Amazon EKS

Você pode configurar parâmetros específicos do seu agente de GuardDuty segurança para o Amazon EKS. Esse suporte está disponível para a versão 1.5.0 e superior do GuardDuty Security Agent. Para obter informações sobre as versões mais recentes do complemento, consulteGuardDuty agente de segurança para clusters Amazon EKS.

Por que devo atualizar o esquema de configuração do agente de segurança?

> O esquema de configuração do agente GuardDuty de segurança é o mesmo em todos os contêineres em seus clusters do Amazon EKS. Quando os valores padrão não estiverem alinhados com as cargas de trabalho e o tamanho da instância associados, considere definir as configurações de CPU, de memória e de configuração. `PriorityClass` `dnsPolicy` Independentemente de como você gerencia o GuardDuty agente para seus clusters do Amazon EKS, você pode configurar ou atualizar a configuração existente desses parâmetros.

Comportamento automatizado de configuração do agente com parâmetros configurados

Quando GuardDuty gerencia o agente de segurança (complemento EKS) em seu nome, ele atualiza o complemento, conforme necessário. GuardDuty definirá o valor dos parâmetros configuráveis como um valor padrão. No entanto, você ainda pode atualizar os parâmetros para o valor desejado. Se isso levar a um conflito, a opção padrão para resolverConflicts é. `None`

Parâmetros e valores configuráveis

Para obter informações sobre as etapas para configurar os parâmetros do complemento, consulte:

- Implantando o agente GuardDuty de segurança ou

- Atualizando o agente de segurança manualmente

As tabelas a seguir fornecem os intervalos e valores que você pode usar para implantar o complemento Amazon EKS manualmente ou atualizar as configurações existentes do complemento.

Configurações da CPU

Parâmetros	Valor padrão	Alcance configurável
Solicitações	200 m	Entre 200m e 10000m, ambos inclusive
Limites	1000 m	

Configurações de memória

Parâmetros	Valor padrão	Alcance configurável
Solicitações	256 milhões	Entre 256Mi e 20000Mi, ambos inclusive
Limites	1024 mi	

Configurações do **`PriorityClass`**

Quando GuardDuty cria um complemento do Amazon EKS para você, o atribuído `PriorityClass` é`aws-guardduty-agent.priorityclass`. Isso significa que nenhuma ação será tomada com base na prioridade do pod do agente. Você pode configurar o escolhendo uma das seguintes `PriorityClass` opções:

Configurável **`PriorityClass`**	Valor do **`preemptionPolicy`**	**`preemptionPolicy`** descrição	Valor do pod
`aws-guardduty-agent.priorityclass`	`Never`	Nenhuma ação	1000000

Configurável **PriorityClass**	Valor do **preemptionPolicy**	**preemptionPolicy** descrição	Valor do pod
`aws-guardduty-agent.priorityclass-high`	`PreemptLowerPriority`	A atribuição desse valor impedirá a execução de um pod com o valor de prioridade menor que o valor do pod do agente.	100000000
`system-cluster-critical` [1]	`PreemptLowerPriority`		2000000000
`system-node-critical` [1]	`PreemptLowerPriority`		2000001000

[1] O Kubernetes fornece essas duas `PriorityClass` opções — e. `system-cluster-critical` `system-node-critical` Para obter mais informações, consulte a PriorityClassdocumentação do Kubernetes.

Configurações do **dnsPolicy**

Escolha uma das seguintes opções de política de DNS compatíveis com o Kubernetes. Quando nenhuma configuração é especificada, `ClusterFirst` é usado como o valor padrão.

- `ClusterFirst`
- `ClusterFirstWithHostNet`
- `Default`

Para obter informações sobre essas políticas, consulte a Política de DNS do Pod na documentação do Kubernetes.

Implantando o agente GuardDuty de segurança

Esta seção descreve como você pode implantar o agente GuardDuty de segurança pela primeira vez em clusters EKS específicos. Antes de prosseguir com esta seção, verifique se você já configurou os

pré-requisitos e ativou o Runtime Monitoring para suas contas. O agente GuardDuty de segurança (complemento EKS) não funcionará se você não ativar o Runtime Monitoring.

Escolha seu método de acesso preferido para implantar o agente de GuardDuty segurança pela primeira vez.

Console

1. Abra o console do Amazon EKS em https://console.aws.amazon.com/eks/home#/clusters.
2. Escolha o Nome do cluster.
3. Escolha a guia Add-ons (Complementos).
4. Escolha Obter mais complementos.
5. Na página Selecionar complementos, escolha Amazon GuardDuty Runtime Monitoring.
6. Use as configurações padrão na página Definir configurações do complemento selecionado. Se o status do seu complemento EKS for Requer ativação, escolha Ativar GuardDuty. Essa ação abrirá o GuardDuty console para configurar o Runtime Monitoring para suas contas.
7. Depois de configurar o Runtime Monitoring para suas contas, volte para o console do Amazon EKS. O Status do seu complemento do EKS deveria ter mudado para Pronto para instalar.
8. (Opcional) Fornecendo o esquema de configuração complementar do EKS

   Para a versão complementar, se você escolher a versão 1.5.0 e superior, o Runtime Monitoring oferece suporte à configuração de parâmetros específicos do agente. GuardDuty Para obter informações sobre intervalos de parâmetros, consulteConfigurar os parâmetros do complemento EKS.

   a. Expanda as configurações opcionais para visualizar os parâmetros configuráveis e seu valor e formato esperados.
   b. Defina os parâmetros. Os valores devem estar no intervalo fornecido emConfigurar os parâmetros do complemento EKS.
   c. Escolha Salvar alterações para criar o complemento com base na configuração avançada.
   d. Para o método de resolução de conflitos, a opção escolhida será usada para resolver um conflito quando você atualizar o valor de um parâmetro para um valor não padrão. Para obter mais informações sobre as opções listadas, consulte ResolveConflicts na Amazon EKS API Reference.

9. Escolha Próximo.
10. Na página Revisar e criar, verifique as rotas e escolha Criar rotas.
11. Navegue de volta aos detalhes do cluster e selecione a guia Recursos.
12. Você pode ver os novos pods com o prefixo aws-guardduty-agent.

API/CLI

Você pode configurar o agente complementar do Amazon EKS (`aws-guardduty-agent`) usando uma das seguintes opções:

- Corra CreateAddonpara sua conta.
-

> **Note**
>
> Para o complemento`version`, se você escolher a versão 1.5.0 e superior, o Runtime Monitoring oferece suporte à configuração de parâmetros específicos do agente. GuardDuty Para ter mais informações, consulte Configurar os parâmetros do complemento EKS.

Use os seguintes valores para os parâmetros de solicitação:

- Em `addonName`, digite `aws-guardduty-agent`.

  Você pode usar o AWS CLI exemplo a seguir ao usar valores configuráveis compatíveis com as versões do complemento v1.5.0 e superiores. Certifique-se de substituir os valores do espaço reservado destacados em vermelho e os `Example.json` associados aos valores configurados.

```
aws eks create-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-
values 'file://example.json'
```

  Example Exemplo.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
```

```
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

- Para obter informações sobre a `addonVersion` compatível, consulte Versões do Kubernetes suportadas pelo agente de segurança GuardDuty .
- Como alternativa, você pode usar AWS CLI. Para obter mais informações, consulte create-addon.

Atualizando o agente de segurança manualmente

Ao gerenciar o agente GuardDuty de segurança manualmente, você é responsável por atualizá-lo para sua conta. Para receber notificações sobre novas versões do agente, você pode assinar um feed RSS no. GuardDuty histórico de lançamento do agente

Você pode atualizar o agente de segurança para a versão mais recente para se beneficiar do suporte e das melhorias adicionais. Se sua versão atual do agente estiver chegando ao fim do suporte padrão, para continuar usando o Runtime Monitoring (ou EKS Runtime Monitoring), você deverá atualizar sua versão atual do agente. Para obter informações sobre as versões de lançamento, consulteGuardDuty agente de segurança para clusters Amazon EKS.

Pré-requisito

Antes de atualizar a versão do agente de segurança, verifique se a versão do agente que você planeja usar agora é compatível com sua versão do Kubernetes. Para ter mais informações, consulte Versões do Kubernetes suportadas pelo agente de segurança GuardDuty .

Console

1. Abra o console do Amazon EKS em https://console.aws.amazon.com/eks/home#/clusters.
2. Escolha o Nome do cluster.
3. Escolha Complementos.

4. Em Complementos, selecione GuardDutyRuntime Monitoring.
5. Escolha Editar para atualizar os detalhes do agente.
6. Na página Configure GuardDuty Runtime Monitoring, atualize os detalhes.
7. (Opcional) Atualização dos parâmetros de configuração do complemento

   Se a versão do complemento EKS for 1.5.0 ou superior, você também poderá atualizar as configurações do complemento.

   a. Expanda Configurações opcionais para ver o esquema de configuração.
   b. Atualize os valores dos parâmetros com base no intervalo fornecido emConfigurar os parâmetros do complemento EKS.
   c. Escolha Salvar alterações para iniciar a atualização.
   d. Para o método de resolução de conflitos, a opção escolhida será usada para resolver um conflito quando você atualizar o valor de um parâmetro para um valor não padrão. Para obter mais informações sobre as opções listadas, consulte ResolveConflicts na Amazon EKS API Reference.

API/CLI

Para atualizar o agente GuardDuty de segurança para seus clusters do Amazon EKS, consulte Atualização de um complemento.

> **Note**
>
> Para o complemento`version`, se você escolher a versão 1.5.0 e superior, o Runtime Monitoring oferece suporte à configuração de parâmetros específicos do agente. GuardDuty Para obter informações sobre intervalos de parâmetros, consulteConfigurar os parâmetros do complemento EKS.

Você pode usar o AWS CLI exemplo a seguir ao usar valores configuráveis compatíveis com as versões do complemento v1.5.0 e superiores. Certifique-se de substituir os valores do espaço reservado destacados em vermelho e os `Example.json` associados aos valores configurados.

```
aws eks update-addon --region us-east-1 --cluster-name myClusterName --addon-
name aws-guardduty-agent --addon-version v1.5.0-eksbuild.1 --configuration-
values 'file://example.json'
```

Example Exemplo.json

```
{
 "priorityClassName": "aws-guardduty-agent.priorityclass-high",
 "dnsPolicy": "Default",
 "resources": {
  "requests": {
   "cpu": "237m",
   "memory": "512Mi"
  },
  "limits": {
   "cpu": "2000m",
   "memory": "2048Mi"
  }
 }
}
```

Se a versão do complemento do Amazon EKS for 1.5.0 ou superior e você tiver configurado o esquema do complemento, poderá verificar se os valores aparecem corretamente ou não no seu cluster. Para ter mais informações, consulte Verificando atualizações do esquema de configuração.

Verificando atualizações do esquema de configuração

Depois de configurar os parâmetros, execute as etapas a seguir para verificar se o esquema de configuração foi atualizado:

1. Abra o console do Amazon EKS em https://console.aws.amazon.com/eks/home#/clusters.
2. No painel de navegação, escolha Clusters.
3. Na página Clusters, selecione o nome do cluster para o qual você deseja verificar as atualizações.
4. Escolha a guia Recursos.
5. No painel Tipos de recursos, em Cargas de trabalho, escolha. DaemonSets
6. Selecione aws-guardduty-agent.
7. Na aws-guardduty-agentpágina, escolha Visualização bruta para ver a resposta JSON não formatada. Verifique se os parâmetros configuráveis exibem o valor que você forneceu.

Depois de verificar, mude para o GuardDuty console. Selecione o correspondente Região da AWS e visualize o status da cobertura dos seus clusters do Amazon EKS. Para ter mais informações, consulte Cobertura para clusters Amazon EKS.

Configurando o EKS Runtime Monitoring (somente API)

Antes de configurar o Monitoramento de runtime do EKS em sua conta, verifique se você está usando uma das plataformas verificadas que oferece suporte à versão do Kubernetes que está em uso no momento. Para saber mais, consulte Validação dos requisitos de arquitetura.

Configuração do Monitoramento de runtime do EKS para uma conta independente

Para as contas associadas ao AWS Organizations, consulte Configuração do Monitoramento de runtime do EKS para ambientes com várias contas.

Escolha seu método de acesso preferido para ativar o Monitoramento de runtime do EKS em sua conta.

API/CLI

Com base nas Abordagens para gerenciar o agente GuardDuty de segurança, você pode escolher uma abordagem preferida e seguir as etapas mencionadas na tabela a seguir.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (monitore todos os clusters EKS)	1. Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizaç ões do agente de segurança para todos os clusters do Amazon EKS em sua conta.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	2. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando a tag de exclusão)	1. Adicione uma tag ao cluster do EKS que você deseja excluir do monitoramento. O par de chave-valor é `GuardDutyManaged -false`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	3. **Note** Sempre adicione a tag de exclusão ao seu cluster EKS antes `STATUS` de `EKS_RUNTIME_MONITORING` definir of como`ENABLED`; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta. Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que não foram excluídos do monitoramento. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` :

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	`aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos (usando a tag de inclusão)	1. Adicione uma tag ao cluster do EKS que você deseja excluir do monitoramento. O par de chave-valor é `GuardDutyManaged -true`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	3. Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que foram marcados com o `true` par `GuardDutyManaged` -. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerenciar o agente de segurança manualmente	1. Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` 2. Para gerenciar o agente de segurança, consulte Gerenciando o agente de segurança manualmente para o cluster Amazon EKS.

Configuração do Monitoramento de runtime do EKS para ambientes com várias contas

Em ambientes com várias contas, somente a conta de GuardDuty administrador delegado pode ativar ou desativar o EKS Runtime Monitoring para as contas dos membros e gerenciar o

gerenciamento de GuardDuty agentes para os clusters EKS pertencentes às contas dos membros em sua organização. As contas GuardDuty dos membros não podem modificar essa configuração em suas contas. A conta de GuardDuty administrador delegado gerencia suas contas de membros usando AWS Organizations. Para obter mais informações sobre ambientes com várias contas, consulte Gerenciar de várias contas.

Configurando o EKS Runtime Monitoring para uma conta de administrador delegado GuardDuty

Escolha seu método de acesso preferido para ativar o EKS Runtime Monitoring e gerenciar o agente de GuardDuty segurança dos clusters EKS que pertencem à conta de GuardDuty administrador delegado.

API/CLI

Com base nas Abordagens para gerenciar o agente GuardDuty de segurança, você pode escolher uma abordagem preferida e seguir as etapas mencionadas na tabela a seguir.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (monitore todos os clusters EKS)	Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS em sua conta. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando a tag de exclusão)	1. Adicione uma tag ao cluster do EKS que você deseja excluir do monitoramento. O par de chave-valor é `GuardDutyManaged -false`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	3. **Note** Sempre adicione a tag de exclusão ao seu cluster EKS antes `STATUS` de `EKS_RUNTIME_MONITORING` definir of como`ENABLED`; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta. Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que não foram excluídos do monitoramento. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` :

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	`aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos (usando a tag de inclusão)	1. Adicione uma tag ao cluster do EKS que você deseja excluir do monitoramento. O par de chave-valor é `GuardDutyManaged -true`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	3. Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que foram marcados com o `true` par `GuardDutyManaged` -. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerenciar o agente de segurança manualmente	1. Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] }]'` 2. Para gerenciar o agente de segurança, consulte Gerenciando o agente de segurança manualmente para o cluster Amazon EKS.

Habilitar automaticamente o Monitoramento de runtime do EKS para todas as contas-membro

Escolha seu método de acesso preferido para habilitar o Monitoramento de runtime do EKS para todas as contas-membro. Isso inclui a conta de GuardDuty administrador delegado, as contas de membros existentes e as novas contas que ingressam na organização. Escolha sua abordagem

preferida para gerenciar o agente de GuardDuty segurança para os clusters EKS que pertencem a essas contas membros.

API/CLI

Com base nas Abordagens para gerenciar o agente GuardDuty de segurança, você pode escolher uma abordagem preferida e seguir as etapas mencionadas na tabela a seguir.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (monitore todos os clusters EKS)	Para habilitar seletivamente o Monitoramento de runtime do EKS para suas contas-membro, execute a operação da API updateMemberDetectors usando seu próprio *ID de detector*. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS em sua conta. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Note Você também pode passar uma lista de IDs de contas separadas por um espaço. Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts` . Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando a tag de exclusão)	1. Adicione uma tag ao cluster do EKS que você deseja excluir do monitoramento. O par de chave-valor é `GuardDuty Managed -false`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** Sempre adicione a tag de exclusão ao seu cluster EKS antes `STATUS` de `EKS_RUNTIME_MONITORING` definir of como`ENABLED`; caso contrário, o

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta. Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que não foram excluídos do monitoramento. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Note Você também pode passar uma lista de IDs de contas separadas por um espaço. Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts` . Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos (usando a tag de inclusão)	1. Adicione uma tag ao cluster do EKS que você deseja excluir do monitoramento. O par de chave-valor é `GuardDuty Managed -true`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:Untag Resource` . • Substitua *access-project* por `GuardDutyManaged` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que foram marcados com o `true` par `GuardDutyManaged` -. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` **Note** Você também pode passar uma lista de IDs de contas separadas por um espaço. Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts` . Se houver algum problema na alteração das configurações do detector de uma

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	conta, esse ID de conta será listado junto com um resumo do problema.
Gerenciar o agente de segurança manualmente	1. Execute a API updateDetector usando seu próprio ID de detector regional e transmitindo o nome de objeto `features` como `EKS_RUNTIME_MONITORING` e o status como `ENABLED`. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. Para gerenciar o agente de segurança, consulte Gerenciando o agente de segurança manualmente para o cluster Amazon EKS.

Configuração do Monitoramento de runtime do EKS para todas as contas-membro ativas existentes

Escolha seu método de acesso preferido para ativar o EKS Runtime Monitoring e gerenciar o agente de GuardDuty segurança para contas de membros ativos existentes em sua organização.

API/CLI

Com base nas Abordagens para gerenciar o agente GuardDuty de segurança, você pode escolher uma abordagem preferida e seguir as etapas mencionadas na tabela a seguir.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (monitore todos os clusters EKS)	Para habilitar seletivamente o Monitoramento de runtime do EKS para suas contas-membro, execute a operação da API updateMemberDetectors usando seu próprio *ID de detector*. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS em sua conta. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Note Você também pode passar uma lista de IDs de contas separadas por um espaço. Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts` . Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando a tag de exclusão)	1. Adicione uma tag ao cluster do EKS que você deseja excluir do monitoramento. O par de chave-valor é `GuardDuty Managed -false`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:Untag Resource` . • Substitua *access-project* por `GuardDutyManaged` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. **Note** Sempre adicione a tag de exclusão ao seu cluster EKS antes `STATUS` de `EKS_RUNTIME_MONITORING` definir of como`ENABLED`; caso contrário, o

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta. Para habilitar seletivamente o Monitoramento de runtime do EKS para suas contas-membro, execute a operação da API updateMemberDetectors usando seu próprio *ID de detector*. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que não foram excluídos do monitoramento. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	> **Note** > Você também pode passar uma lista de IDs de contas separadas por um espaço. Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts` . Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos (usando a tag de inclusão)	1. Adicione uma tag ao cluster do EKS que você deseja excluir do monitoramento. O par de chave-valor é `GuardDuty Managed -true`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *`ec2: CreateTags`* por `eks:TagResource` . • Substitua *`ec2: DeleteTags`* por `eks:UntagResource` . • Substitua *`access-project`* por `GuardDutyManaged` • Substitua *`123456789012`* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável, use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]` 3. Para habilitar seletivamente o Monitoramento de runtime do EKS para suas contas-membro, execute a operação da API updateMemberDetectors usando seu próprio *`ID de detector`*.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que foram marcados com o `true` par `GuardDutyManaged` -. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'` **Note** Você também pode passar uma lista de IDs de contas separadas por um espaço. Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts` . Se houver algum problema na alteração das configurações do detector de uma

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	conta, esse ID de conta será listado junto com um resumo do problema.
Gerenciar o agente de segurança manualmente	1. Para habilitar seletivamente o Monitoramento de runtime do EKS para suas contas-membro, execute a operação da API updateMemberDetectors usando seu próprio *ID de detector*. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : " ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. Para gerenciar o agente de segurança, consulte Gerenciando o agente de segurança manualmente para o cluster Amazon EKS.

Habilitar automaticamente o Monitoramento de runtime do EKS para novos membros

A conta de GuardDuty administrador delegado pode ativar automaticamente o EKS Runtime Monitoring e escolher uma abordagem de como gerenciar o agente de GuardDuty segurança para novas contas que ingressam na sua organização.

API/CLI

Com base nas Abordagens para gerenciar o agente GuardDuty de segurança, você pode escolher uma abordagem preferida e seguir as etapas mencionadas na tabela a seguir.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (monitore todos os clusters EKS)	Para habilitar seletivamente o Monitoramento de runtime do EKS para suas novas contas, invoque a operação da API UpdateOrganizationConfiguration usando seu próprio *ID de detector*. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS em sua conta. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` para uma única conta. Você também pode passar uma lista de IDs de contas separadas por um espaço.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando a tag de exclusão)	1. Adicione uma tag ao cluster do EKS que você deseja excluir do monitoramento. O par de chave-valor é `GuardDutyManaged -false`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	3. **Note** Sempre adicione a tag de exclusão ao seu cluster EKS antes `STATUS` de `EKS_RUNTIME_MONITORING` definir of como`ENABLED`; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta. Para habilitar seletivamente o Monitoramento de runtime do EKS para suas novas contas, invoque a operação da API UpdateOrganizationConfiguration usando seu próprio *`ID de detector`*. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que não foram excluídos do monitoramento. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` para uma única conta. Você também pode passar uma lista de IDs de contas separadas por um espaço.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos (usando a tag de inclusão)	1. Adicione uma tag ao cluster do EKS que você deseja excluir do monitoramento. O par de chave-valor é `GuardDutyManaged -true`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	3. Para habilitar seletivamente o Monitoramento de runtime do EKS para suas novas contas, invoque a operação da API UpdateOrganizationConfiguration usando seu próprio *ID de detector*. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. GuardDuty gerenciará a implantação e as atualizaç ões do agente de segurança para todos os clusters do Amazon EKS que foram marcados com o `true` par `GuardDutyManaged` -. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configura ções no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITO RING` e desabilita `EKS_ADDON_MANAGEMENT` para uma única conta. Você também pode passar uma lista de IDs de contas separadas por um espaço. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configura ções no console https://console.aws.amazon.com/guardduty/. `aws guardduty update-organization-configu ration --detector-id 12abc34d567e8fa901 bc2d34e56789f0 --autoEnable --feature s '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfigu`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	ration" : [{"Name" : "EKS_ADDON_MANAGEM ENT", "AutoEnable": "NEW"}]]' Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts` . Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerenciar o agente de segurança manualmente	1. Para habilitar seletivamente o Monitoramento de runtime do EKS para suas novas contas, invoque a operação da API UpdateOrganizationConfiguration usando seu próprio *ID de detector*. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` para uma única conta. Você também pode passar uma lista de IDs de contas separadas por um espaço. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. `aws guardduty update-organization-configuration --detector-id 12abc34d567e8fa901bc2d34e56789f0 --autoEnable --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NEW", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "AutoEnable": "NEW"}] ]'` Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema. 2. Para gerenciar o agente de segurança, consulte Gerenciando o agente de segurança manualmente para o cluster Amazon EKS.

Habilitar o Monitoramento de runtime do EKS para contas-membro individuais ativas

API/CLI

Com base nas Abordagens para gerenciar o agente GuardDuty de segurança, você pode escolher uma abordagem preferida e seguir as etapas mencionadas na tabela a seguir.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerencie o agente de segurança por meio de GuardDuty (monitore todos os clusters EKS)	Para habilitar seletivamente o Monitoramento de runtime do EKS para suas contas-membro, execute a operação da API updateMemberDetectors usando seu próprio *ID de detector*. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS em sua conta. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : "ENABLED"}] ]'` **Note** Você também pode passar uma lista de IDs de contas separadas por um espaço. Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts` . Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar todos os clusters do EKS, mas excluir alguns deles (usando a tag de exclusão)	1. Adicione uma tag ao cluster do EKS que você deseja excluir do monitoramento. O par de chave-valor é `GuardDutyManaged -false`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	3. **Note** Sempre adicione a tag de exclusão ao seu cluster EKS antes `STATUS` de `EKS_RUNTIME_MONITORING` definir of como`ENABLED`; caso contrário, o agente de GuardDuty segurança será implantado em todos os clusters EKS em sua conta. Para habilitar seletivamente o Monitoramento de runtime do EKS para suas contas-membro, execute a operação da API updateMemberDetectors usando seu próprio *`ID de detector`*. Defina o status de `EKS_ADDON_MANAGEMENT` como `ENABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que não foram excluídos do monitoramento. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e `EKS_ADDON_MANAGEMENT` :

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	`aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] ]'` **Note** Você também pode passar uma lista de IDs de contas separadas por um espaço. Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts` . Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Monitorar clusters do EKS seletivos (usando a tag de inclusão)	1. Adicione uma tag ao cluster do EKS que você deseja excluir do monitoramento. O par de chave-valor é `GuardDutyManaged -true`. Para obter mais informações sobre como adicionar a tag Como trabalhar com tags usando a CLI, a API ou o eksctl no Guia do usuário do Amazon EKS. 2. Para evitar a modificação de tags, exceto pelas entidades confiáveis, use a política fornecida em Impedir que as tags sejam modificadas, exceto por diretores autorizados no Guia do usuário do AWS Organizations . Nessa política, substitua estes detalhes: • Substitua *ec2: CreateTags* por `eks:TagResource` . • Substitua *ec2: DeleteTags* por `eks:UntagResource` . • Substitua *access-project* por `GuardDutyManaged` • Substitua *123456789012* pela ID da Conta da AWS entidade confiável. Quando você tiver mais de uma entidade confiável , use o exemplo a seguir para adicionar vários `PrincipalArn` : `"aws:PrincipalArn":["arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin", "arn:aws:iam::123456789012:role/org-admins/iam-admin"]`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	3. Para habilitar seletivamente o Monitoramento de runtime do EKS para suas contas-membro, execute a operação da API updateMemberDetectors usando seu próprio *ID de detector*. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. GuardDuty gerenciará a implantação e as atualizações do agente de segurança para todos os clusters do Amazon EKS que foram marcados com o `true` par `GuardDutyManaged` -. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " DISABLED"}] ]'`

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
	> **Note** > Você também pode passar uma lista de IDs de contas separadas por um espaço. Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts` . Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Abordagem preferida para gerenciar o agente GuardDuty de segurança	Etapas
Gerenciar o agente de segurança manualmente	1. Para habilitar seletivamente o Monitoramento de runtime do EKS para suas contas-membro, execute a operação da API updateMemberDetectors usando seu próprio *ID de detector*. Defina o status de `EKS_ADDON_MANAGEMENT` como `DISABLED`. Como alternativa, você pode usar o AWS CLI comando usando seu próprio ID de detector regional. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/. O exemplo a seguir habilita `EKS_RUNTIME_MONITORING` e desabilita `EKS_ADDON_MANAGEMENT` : `aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 555555555555 --features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "ENABLED", "AdditionalConfiguration" : [{"Name" : "EKS_ADDON_MANAGEMENT", "Status" : " ENABLED"}] } ]'` 2. Para gerenciar o agente de segurança, consulte Gerenciando o agente de segurança manualmente para o cluster Amazon EKS.

Migração do monitoramento de tempo de execução do EKS para o monitoramento de tempo de execução

Com o lançamento do GuardDuty Runtime Monitoring, a cobertura de detecção de ameaças foi expandida para contêineres do Amazon ECS e instâncias do Amazon EC2. O EKS Runtime Monitoring agora foi consolidado no Runtime Monitoring. Você pode ativar o Runtime Monitoring e gerenciar agentes de GuardDuty segurança individuais para cada tipo de recurso (instância do Amazon EC2, cluster do Amazon ECS e cluster do Amazon EKS) para o qual você deseja monitorar o comportamento do tempo de execução.

Não há uma experiência de GuardDuty console separada para o EKS Runtime Monitoring. Para continuar usando o EKS Runtime Monitoring, você precisa configurá-lo usando APIs ou o. AWS Command Line Interface

Para migrar do EKS Runtime Monitoring para o Runtime Monitoring

1. O GuardDuty console oferece suporte ao EKS Runtime Monitoring como parte do Runtime Monitoring.

   Você pode começar a usar o Runtime Monitoring por meio Verificando o status da configuração do EKS Runtime Mon de sua organização e contas.

   Certifique-se de não desativar o EKS Runtime Monitoring antes de ativar o Runtime Monitoring. Se você desativar o EKS Runtime Monitoring, o gerenciamento de complementos do Amazon EKS também será desativado. Continue com as etapas a seguir na ordem listada.
2. Certifique-se de conhecer todos osPré-requisitos para habilitar o monitoramento de tempo de execução.
3. Ative o Runtime Monitoring replicando as mesmas configurações da organização para o Runtime Monitoring que você tem para o EKS Runtime Monitoring. Para ter mais informações, consulte Habilitando o monitoramento de tempo.
   - Se você tiver uma conta independente, precisará ativar o Runtime Monitoring.

     Se seu agente GuardDuty de segurança já estiver implantado, as configurações correspondentes serão replicadas automaticamente e você não precisará defini-las novamente.
   - Se você tiver uma organização com configurações de ativação automática, certifique-se de replicar as mesmas configurações de ativação automática para o Runtime Monitoring.

- Se você tiver uma organização com configurações definidas individualmente para contas de membros ativos existentes, certifique-se de ativar o Runtime Monitoring e configurar o agente de GuardDuty segurança para esses membros individualmente.

4. Depois de garantir que as configurações do Runtime Monitoring e do agente de GuardDuty segurança estejam corretas, desative o EKS Runtime Monitoring usando a API ou o AWS CLI comando.
5. (Opcional) se você quiser limpar qualquer recurso associado ao agente GuardDuty de segurança, consulteLimpando os recursos do agente de GuardDuty segurança.

Se você quiser continuar usando o EKS Runtime Monitoring sem habilitar o Runtime Monitoring, consulteConfigurando o EKS Runtime Monitoring (somente API).

Verificando o status da configuração do EKS Runtime Mon

Use as seguintes APIs ou AWS CLI comandos para verificar o status da configuração existente do EKS Runtime Monitoring.

Para verificar o status da configuração existente do EKS Runtime Monitoring em sua conta

- Execute GetDetectorpara verificar o status da configuração da sua própria conta.
- Como alternativa, você pode executar o seguinte comando usando AWS CLI:

```
aws guardduty get-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
region us-east-1
```

Certifique-se de substituir o ID do detector da sua região Conta da AWS e da atual. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

Para verificar o status da configuração existente do EKS Runtime Monitoring para sua organização (somente como uma conta de GuardDuty administrador delegada)

- Execute DescribeOrganizationConfigurationpara verificar o status da configuração da sua organização.

  Como alternativa, você pode executar o seguinte comando usando AWS CLI:

```
aws guardduty describe-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --region us-east-1
```

Certifique-se de substituir o ID do detector pelo ID do detector da sua conta de GuardDuty administrador delegado e a Região pela sua região atual. Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

Desativando o EKS Runtime Monitoring após migrar para o Runtime Monitoring

Depois de garantir que as configurações existentes da sua conta ou organização tenham sido replicadas para o Runtime Monitoring, você pode desativar o EKS Runtime Monitoring.

Para desativar o EKS Runtime Monitoring

- Para desativar o EKS Runtime Monitoring em sua própria conta

  Execute a UpdateDetectorAPI com seu próprio *detector-id* regional.

  Como alternativa, você pode usar o AWS CLI comando a seguir. *Substitua 12abc34d567e8fa901bc2d34e56789f0 por sua própria identificação de detector regional.*

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "EKS_RUNTIME_MONITORING", "Status" : "DISABLED"}]'
```

- Para desativar o EKS Runtime Monitoring para contas de membros em sua organização

  Execute a UpdateMemberDetectorsAPI com o *detector-id* regional da conta de GuardDuty administrador delegado da organização.

  Como alternativa, você pode usar o AWS CLI comando a seguir. *Substitua 12abc34d567e8fa901bc2d34e56789f0 pelo ID do detector regional da conta de administrador delegado da organização e 111122223333 pelo ID da conta membro para a qual você deseja desativar esse recurso. GuardDuty* Conta da AWS

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 111122223333 --features '[{"Name" : "EKS_RUNTIME_MONITORING",
 "Status" : "DISABLED"}]'
```

- Para atualizar as configurações de ativação automática do EKS Runtime Monitoring para sua organização

  Execute a etapa a seguir somente se você tiver configurado as configurações de ativação automática do EKS Runtime Monitoring para contas novas (`NEW`) ou todas (`ALL`) membros na organização. Se você já o configurou como`NONE`, pode pular esta etapa.

  > **Note**
  >
  > Definir a configuração de ativação automática do EKS Runtime Monitoring como `NONE` significa que o EKS Runtime Monitoring não será ativado automaticamente para nenhuma conta membro existente ou quando uma nova conta membro ingressar na sua organização.

  Execute a UpdateOrganizationConfigurationAPI com o *`detector-id`* regional da conta de GuardDuty administrador delegado da organização.

  Como alternativa, você pode usar o AWS CLI comando a seguir. *`Substitua 12abc34d567e8fa901bc2d34e56789f0 pelo ID do detector regional da conta de administrador delegado da organização.`* GuardDuty Substitua o *`EXISTING_VALUE`* pela sua configuração atual para ativação automática. GuardDuty

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members EXISTING_VALUE
   --features '[{"Name" : "EKS_RUNTIME_MONITORING", "AutoEnable": "NONE"}]'
  ```

Limpando os recursos do agente de GuardDuty segurança

É possível limpar os recursos nos seguintes cenários:

Quando você desativa a configuração automatizada do agente

GuardDuty não remove o agente de segurança que está implantado em seu recurso. No entanto, GuardDuty deixará de gerenciar as atualizações do agente de segurança.

GuardDuty continua recebendo os eventos de tempo de execução do seu tipo de recurso. Para evitar um impacto nas estatísticas de uso, certifique-se de remover o agente de GuardDuty segurança do seu recurso.

Se um usuário Conta da AWS usa ou não um VPC endpoint compartilhado, GuardDuty isso não exclui o VPC endpoint. Se necessário, você precisará excluir o VPC endpoint manualmente.

Quando você desabilita o Runtime Monitoring ou o EKS Runtime

Em geral, GuardDuty exclui o VPC endpoint que ele criou. GuardDuty os marca como`GuardDutyManaged:true`. No entanto, quando você desativa o Runtime Monitoring ou o EKS Runtime Monitoring para uma conta compartilhada de participante da VPC, se o endpoint da VPC compartilhada tiver sido usado por pelo menos uma conta participante, nem GuardDuty o endpoint da VPC nem o grupo de segurança associado ao recurso da VPC compartilhada.

Quando você para de gerenciar o agente de segurança manualmente

Independentemente da abordagem usada para implantar e gerenciar o agente de GuardDuty segurança, para parar de monitorar os eventos de tempo de execução em seu recurso, você deve remover o agente GuardDuty de segurança. Quando quiser parar de monitorar os eventos de tempo de execução de um tipo de recurso em uma conta, você também pode excluir o endpoint da Amazon VPC.

Processo para limpar os recursos do agente de segurança

Para excluir o endpoint da Amazon VPC

- Sem uma VPC compartilhada — Quando você não quiser mais monitorar um recurso em uma conta, considere excluir o endpoint da Amazon VPC.
- Com uma VPC compartilhada — Quando a conta do proprietário da VPC compartilhada exclui o recurso da VPC compartilhada, qualquer conta participante que esteja usando atualmente o endpoint da VPC compartilhada, o status da cobertura do Runtime Monitoring para os recursos na sua conta de proprietário da VPC compartilhada e na conta participante pode ficar insalubre. Para ter mais informações, consulte Avaliando a cobertura de tempo de execução de seus recursos.

Para obter mais informações, consulte Excluir um endpoint de interface.

Para excluir o grupo de segurança

- Sem uma VPC compartilhada — Quando você não quiser mais monitorar um tipo de recurso em uma conta, considere excluir o grupo de segurança associado à Amazon VPC.
- Com uma VPC compartilhada — Quando a conta do proprietário da VPC compartilhada exclui o grupo de segurança, qualquer conta de participante que esteja usando atualmente o grupo de segurança associado à VPC compartilhada, o status da cobertura do Runtime Monitoring para os recursos na sua conta de proprietário da VPC compartilhada e na conta participante pode ficar insalubre. Para ter mais informações, consulte Avaliando a cobertura de tempo de execução de seus recursos.

Para obter mais informações, consulte Excluir um grupo de segurança.

Para remover o agente de GuardDuty segurança de um cluster EKS

Para remover o agente de segurança do cluster EKS que você não deseja mais monitorar, consulte Excluindo um complemento.

A remoção do agente complementar do EKS não remove o namespace `amazon-guardduty` do cluster do EKS. Para excluir o namespace `amazon-guardduty`, consulte Deleting a namespace.

Para excluir o **`amazon-guardduty`** namespace (cluster EKS)

Desativar a configuração automatizada do agente não remove automaticamente o `amazon-guardduty` namespace do seu cluster EKS. Para excluir o namespace `amazon-guardduty`, consulte Deleting a namespace.

Avaliando a cobertura de tempo de execução de seus recursos

Depois de habilitar o Runtime Monitoring e o agente de GuardDuty segurança ser implantado em seu recurso, GuardDuty fornece estatísticas de cobertura para o tipo de recurso correspondente e status de cobertura individual para os recursos que pertencem à sua conta. O status da cobertura é determinado pela garantia de que você habilitou o Runtime Monitoring, que seu endpoint Amazon VPC foi criado e que o agente de GuardDuty segurança do recurso correspondente foi implantado. Um status de cobertura saudável indica que, quando há um evento de tempo de execução relacionado ao seu recurso, GuardDuty é capaz de receber esse evento de tempo de execução por meio do endpoint da Amazon VPC e monitorar o comportamento. Se houve um problema no momento da configuração do Runtime Monitoring, da criação de um endpoint da Amazon VPC ou da implantação do agente de segurança, GuardDuty o status da cobertura aparecerá como Não íntegro.

Quando o status da cobertura não estiver íntegro, não GuardDuty poderá receber ou monitorar o comportamento de tempo de execução do recurso correspondente nem gerar nenhuma descoberta do Runtime Monitoring.

Os tópicos a seguir ajudarão você a analisar as estatísticas de cobertura, configurar EventBridge notificações e solucionar os problemas de cobertura de um tipo específico de recurso.

Conteúdo

Cobertura para a instância do Amazon EC2

Para um recurso do Amazon EC2, a cobertura do tempo de execução é avaliada no nível da instância. Suas instâncias do Amazon EC2 podem executar vários tipos de aplicativos e cargas de trabalho, entre outros, em seu ambiente. AWS Esse recurso também suporta instâncias do Amazon EC2 gerenciadas pelo Amazon EC2 e, se você tiver clusters do Amazon ECS em execução em uma instância do Amazon EC2, os problemas de cobertura no nível da instância aparecerão na cobertura de tempo de execução do Amazon EC2.

Tópicos

Análise de estatísticas de cobertura

As estatísticas de cobertura das instâncias do Amazon EC2 associadas às suas próprias contas ou às suas contas membros são a porcentagem das instâncias do EC2 saudáveis em relação a todas as instâncias do EC2 nas selecionadas. Região da AWS A seguinte equação representa isso como:

(Instâncias ínteis/todas as instâncias) *100

Se você também implantou o agente de GuardDuty segurança para seus clusters do Amazon ECS, qualquer problema de cobertura no nível da instância associado aos clusters do Amazon ECS

executados em uma instância do Amazon EC2 aparecerá como um problema de cobertura de tempo de execução da instância do Amazon EC2.

Selecione um dos métodos de acesso para revisar as estatísticas de cobertura de suas contas.

Console

- Faça login no AWS Management Console e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
- No painel de navegação, escolha Runtime Monitoring.
- Escolha a guia Cobertura de tempo de execução.
- Na guia Cobertura de tempo de execução da instância EC2, você pode visualizar as estatísticas de cobertura agregadas pelo status de cobertura de cada instância do Amazon EC2 que está disponível na tabela da lista de instâncias.
  - Você pode filtrar a tabela da lista de instâncias pelas seguintes colunas:
    - ID da conta
    - Tipo de gerenciamento de agentes
    - Versão do agente
    - Status da cobertura
    - ID da instância
    - ARN do cluster
- Se alguma de suas instâncias do EC2 tiver o status de Cobertura como Não íntegra, a coluna Problema incluirá informações adicionais sobre o motivo do status Não íntegro.

API/CLI

- Execute a ListCoverageAPI com seu próprio ID de detector válido, região atual e endpoint de serviço. Você pode filtrar e classificar a lista de instâncias usando essa API.
  - Você pode alterar o `filter-criteria` de exemplo com uma das seguintes opções para `CriterionKey`:
    - `ACCOUNT_ID`
    - `RESOURCE_TYPE`
    - `COVERAGE_STATUS`
    - `AGENT_VERSION`

    - MANAGEMENT_TYPE
    - INSTANCE_ID
    - CLUSTER_ARN
  - Quando `filter-criteria` incluído RESOURCE_TYPE como EC2, o Runtime Monitoring não suporta o uso de ISSUE como o. `AttributeName` Se você usá-lo, a resposta da API resultará em`InvalidInputException`.

    Você pode alterar o `AttributeName` de exemplo em `sort-criteria` com uma das seguintes opções:

    - ACCOUNT_ID
    - COVERAGE_STATUS
    - INSTANCE_ID
    - UPDATED_AT
  - Você pode alterar *`max-results`* (até 50).
  - Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Execute a GetCoverageStatisticsAPI para recuperar estatísticas agregadas de cobertura com base no. `statisticsType`
  - Você pode alterar o `statisticsType` de exemplo com uma das seguintes opções:
    - COUNT_BY_COVERAGE_STATUS: representa estatísticas de cobertura para clusters do EKS agregadas por status de cobertura.
    - COUNT_BY_RESOURCE_TYPE— Estatísticas de cobertura agregadas com base no tipo de AWS recurso na lista.
    - Você pode alterar o `filter-criteria` de exemplo no comando. É possível usar as seguintes opções para `CriterionKey`:
      - ACCOUNT_ID
      - RESOURCE_TYPE

  - `COVERAGE_STATUS`
  - `AGENT_VERSION`
  - `MANAGEMENT_TYPE`
  - `INSTANCE_ID`
  - `CLUSTER_ARN`
- Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Se o status da cobertura da sua instância do EC2 for Insalubre, consulte. Solução de problemas de cobertura

Configuração de notificações de alteração do status de cobertura

O status da cobertura da sua instância do Amazon EC2 pode aparecer como Insalubre. Para saber quando o status da cobertura muda, recomendamos que você monitore o status da cobertura periodicamente e solucione problemas se o status ficar insalubre. Como alternativa, você pode criar uma EventBridge regra da Amazon para receber uma notificação quando o status da cobertura mudar de Insalubre para Saudável ou não. Por padrão, GuardDuty publica isso no EventBridge barramento da sua conta.

Exemplo de esquema de notificação

Em uma EventBridge regra, você pode usar os exemplos de eventos e padrões de eventos predefinidos para receber a notificação do status da cobertura. Para obter mais informações sobre a criação de uma EventBridge regra, consulte Criar regra no Guia EventBridge do usuário da Amazon.

Além disso, você pode criar um padrão de evento personalizado usando o exemplo de esquema de notificação a seguir. Substitua os valores da sua conta. Para ser notificado quando o status da cobertura da sua instância do Amazon EC2 mudar de `Healthy` para`Unhealthy`, a opção `detail-type` deve ser *`GuardDuty Runtime Protection Unhealthy`*. Para ser notificado quando o status da cobertura mudar de `Unhealthy` para`Healthy`, substitua o valor de `detail-type` por *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Conta da AWS ID",
  "time": "event timestamp (string)",
  "region": "Região da AWS",
  "resources": [
      ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EC2",
        "ec2InstanceDetails": {
          "instanceId":"",
          "instanceType":"",
          "clusterArn": "",
          "agentDetails": {
            "version":""
          },
          "managementType":""
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Solução de problemas de cobertura

Se o status da cobertura da sua instância do Amazon EC2 for Insalubre, você poderá ver o motivo na coluna Problema.

A tabela a seguir lista os tipos de problemas e as etapas de solução de problemas correspondentes.

Tipo de problema	Mensagem de emissão	Etapas de solução de problemas
Sem relatórios de agentes	Aguardando a notificação do SSM	Certifique-se de que a instância do Amazon EC2 já seja gerenciada por SSM. O recebimento da notificação de SSM pode levar alguns minutos.
	(Vazio de propósito)	Se você estiver gerenciando o agente GuardDuty de segurança manualmente, isso não é acionável.
		Se você ativou a configuração automática do agente: • Sua instância EC2 é gerenciada por SSM. • Visualize o status do seu agente de segurança periodicamente. Para ter mais informações, consulte Validando o status GuardDuty de instalação do agente de segurança.
	Agente desconectado	• Veja o status do seu agente de segurança. Para ter mais informações, consulte Validando o status GuardDuty de instalação do agente de segurança. • Visualize os registros do agente de segurança para identificar a possível causa raiz. Os registros fornecem erros detalhados que você pode usar para solucionar o problema sozinho. Os arquivos de log estão disponíveis em `/var/log/amzn-guardduty-agent/` . Faça `sudo journalctl -u amazon-guardduty-agent`
Falha na criação da associação SSM	GuardDuty A associação SSM já existe em sua conta	1. Exclua a associação existente manualmente. Para obter mais informações, consulte Excluindo associações no Guia do AWS Systems Manager usuário. 2. Depois de excluir a associação, desative e reative a configuração GuardDuty automática do agente para o Amazon EC2.

Tipo de problema	Mensagem de emissão	Etapas de solução de problemas
	Sua conta tem muitas associações de SSM	Escolha uma das duas opções a seguir: • Exclua todas as associações SSM não utilizadas. Para obter mais informações, consulte Excluindo associações no Guia do AWS Systems Manager usuário. • Verifique se sua conta está qualificada para um aumento de cota. Para obter mais informações, consulte as cotas do Systems Manager Service no Referência geral da AWS.
Falha na atualização da associação SSM	GuardDuty A associação SSM não existe em sua conta	A associação SSM está ausente. Desative e reative o Runtime Monitoring.
Falha na exclusão da associação SSM	GuardDuty A associação SSM não existe em sua conta	A associação SSM está ausente. Isso não é acionável.

Tipo de problema	Mensagem de emissão	Etapas de solução de problemas
Falha na execução da associação de instância SSM	Os requisitos arquitetônicos ou outros pré-requisitos não são atendidos.	Para obter informações sobre distribuições verificadas do sistema operacional, consulte Pré-requisitos para suporte à instância do Amazon EC2. Se você ainda tiver esse problema, as etapas a seguir ajudarão você a identificar e potencialmente resolver o problema: 1. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/. 2. No painel de navegação, em Gerenciamento de nós, selecione State Manager. 3. Filtre pela propriedade Nome do documento e insira AmazonGuardDuty-ConfigureRuntimeMonitoringSsmPlugin. 4. Selecione o ID da associação correspondente e visualize seu histórico de execução. 5. Usando o histórico de execução, visualize as falhas, identifique a possível causa raiz e tente resolvê-la.
Falha na criação do VPC Endpoint	A criação de endpoints da VPC não é compatível com *vpcId* de VPC compartilhada	O Runtime Monitoring suporta o uso de uma VPC compartilhada em uma organização. Para ter mais informações, consulte Usando VPC compartilhada com agentes de segurança automatizados.

Tipo de problema	Mensagem de emissão	Etapas de solução de problemas
	Somente ao usar VPC compartilhada com configuração automatizada de agentes ID da conta do proprietário *111122223333 para* VPC compartilhada O VPCid não tem o *Runtime Monitoring, a configuração* automatizada do agente ou ambos ativados	A conta compartilhada do proprietário da VPC deve habilitar o Runtime Monitoring e a configuração automática do agente para pelo menos um tipo de recurso (Amazon EKS ou Amazon ECS ())AWS Fargate. Para ter mais informações, consulte Pré-requisitos específicos para o monitoramento de tempo de execução GuardDuty.

Tipo de problema	Mensagem de emissão	Etapas de solução de problemas
	A habilitação do DNS privado requer os atributos da VPC enableDnsSupport e enableDnsHostnames definidos como true para vpcId (Serviço: Ec2, Código de status: 400, ID da solicitação: a1b2c3d4-5678-90ab-cdef-EXAMPLE11111).	Verifique se os seguintes atributos da VPC estão definidos como `true`: `enableDnsSupport` e `enableDnsHostnames` . Para obter mais informações, consulte Atributos de DNS na sua VPC. Se você estiver usando o console da Amazon VPC em https://console.aws.amazon.com/vpc/ para criar a Amazon VPC, certifique-se de selecionar Habilitar nomes de host DNS e Habilitar resolução de DNS. Para obter mais informações, consulte Opções de configuração da VPC.

Tipo de problema	Mensagem de emissão	Etapas de solução de problemas
Falha na exclusão do VPC Endpoint compartilhado	*A exclusão compartilhada do VPC endpoint não é permitida para a ID da conta 111122223333 , VPC compartilhada VPCid, ID da conta do proprietário 555555555555.*	Etapas potenciais: • A desativação do status do Runtime Monitoring da conta compartilhada do participante da VPC não afeta a política de endpoint da VPC compartilhada e o grupo de segurança que existe na conta do proprietário. Para excluir o endpoint e o grupo de segurança da VPC compartilhados, você deve desativar o Runtime Monitoring ou o status de configuração automática do agente na conta compartilhada do proprietário da VPC. • A conta compartilhada do participante da VPC não pode excluir o endpoint e o grupo de segurança da VPC compartilhados hospedados na conta compartilhada do proprietário da VPC.
Agente que não está reportando	(Vazio de propósito)	O tipo de problema chegou ao fim do suporte. Se você continuar enfrentando esse problema e ainda não o fez, habilite o agente GuardDuty automatizado para o Amazon EC2. Se o problema persistir, considere desativar o Runtime Monitoring por alguns minutos e depois habilitá-lo novamente.

Cobertura para o recurso Fargate (somente Amazon ECS)

Para um cluster do Amazon ECS executado no Fargate, a cobertura do tempo de execução é avaliada no nível da tarefa. A cobertura de tempo de execução dos clusters ECS inclui as tarefas do Fargate que começaram a ser executadas depois que você ativou o Runtime Monitoring e a configuração automatizada do agente.

Se sua tarefa do Fargate já estava em execução quando você ativou o Runtime Monitoring, essa tarefa não será considerada para avaliar a cobertura de tempo de execução dos clusters ECS. Para incluir essa tarefa do Fargate, você precisará interromper a tarefa e executá-la novamente.

Análise de estatísticas de cobertura

As estatísticas de cobertura dos recursos AWS Fargate (somente do Amazon ECS) associados às suas próprias contas ou às suas contas membros são a porcentagem dos clusters saudáveis do Amazon ECS em relação a todos os clusters do Amazon ECS selecionados. Região da AWS A seguinte equação representa isso como:

(Clusters íntegros/todos os clusters)*100

As estatísticas de cobertura incluem as tarefas do Fargate que estão em execução ou que terminaram de ser executadas recentemente.

Selecione um dos métodos de acesso para revisar as estatísticas de cobertura de suas contas.

Console

- Faça login no AWS Management Console e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
- No painel de navegação, escolha Runtime Monitoring.
- Escolha a guia Cobertura de tempo de execução.
- Na guia de cobertura de tempo de execução dos clusters do ECS, você pode visualizar as estatísticas de cobertura agregadas pelo status da cobertura de cada cluster do Amazon ECS que está disponível na tabela da lista de clusters.
  - Você pode filtrar a tabela da lista de clusters pelas seguintes colunas:
    - ID da conta
    - Nome do cluster
    - Tipo de gerenciamento de agentes
    - Status da cobertura
- Se algum dos seus clusters do ECS tiver o status de Cobertura como Não íntegro, a coluna Problema incluirá informações adicionais sobre o motivo do status Não íntegro.

API/CLI

- Execute a ListCoverageAPI com seu próprio ID de detector válido, região atual e endpoint de serviço. Você pode filtrar e classificar a lista de instâncias usando essa API.
  - Você pode alterar o `filter-criteria` de exemplo com uma das seguintes opções para `CriterionKey`:
    - `ACCOUNT_ID`
    - `ECS_CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `MANAGEMENT_TYPE`
  - Você pode alterar o `AttributeName` de exemplo em `sort-criteria` com uma das seguintes opções:
    - `ACCOUNT_ID`
    - `COVERAGE_STATUS`
    - `ISSUE`
    - `ECS_CLUSTER_NAME`
    - `UPDATED_AT`

      O campo é atualizado somente quando uma nova tarefa é criada no cluster associado do Amazon ECS ou quando há uma alteração no status de cobertura correspondente.
  - Você pode alterar *`max-results`* (até 50).
  - Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "ECS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Execute a GetCoverageStatisticsAPI para recuperar estatísticas agregadas de cobertura com base no. `statisticsType`
  - Você pode alterar o `statisticsType` de exemplo com uma das seguintes opções:
    - `COUNT_BY_COVERAGE_STATUS`— Representa estatísticas de cobertura para clusters ECS agregadas por status de cobertura.

  - `COUNT_BY_RESOURCE_TYPE`— Estatísticas de cobertura agregadas com base no tipo de AWS recurso na lista.
  - Você pode alterar o `filter-criteria` de exemplo no comando. É possível usar as seguintes opções para `CriterionKey`:
    - `ACCOUNT_ID`
    - `ECS_CLUSTER_NAME`
    - `COVERAGE_STATUS`
    - `MANAGEMENT_TYPE`
    - `INSTANCE_ID`
- Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Para obter mais informações sobre problemas de cobertura, consulteSolução de problemas de cobertura.

Configuração de notificações de alteração do status de cobertura

O status da cobertura do seu cluster Amazon ECS pode aparecer como Não íntegro. Para saber quando o status da cobertura muda, recomendamos que você monitore o status da cobertura periodicamente e solucione problemas se o status ficar insalubre. Como alternativa, você pode criar uma EventBridge regra da Amazon para receber uma notificação quando o status da cobertura mudar de Insalubre para Saudável ou não. Por padrão, GuardDuty publica isso no EventBridge barramento da sua conta.

Exemplo de esquema de notificação

Em uma EventBridge regra, você pode usar os exemplos de eventos e padrões de eventos predefinidos para receber a notificação do status da cobertura. Para obter mais informações sobre a criação de uma EventBridge regra, consulte Criar regra no Guia EventBridge do usuário da Amazon.

Além disso, você pode criar um padrão de evento personalizado usando o exemplo de esquema de notificação a seguir. Substitua os valores da sua conta. Para ser notificado quando o status da

cobertura do seu cluster do Amazon ECS mudar de `Healthy` para`Unhealthy`, a opção `detail-type` deve ser *`GuardDuty Runtime Protection Unhealthy`*. Para ser notificado quando o status da cobertura mudar de `Unhealthy` para`Healthy`, substitua o valor de `detail-type` por *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Conta da AWS ID",
  "time": "event timestamp (string)",
  "region": "Região da AWS",
  "resources": [
      ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "ECS",
        "ecsClusterDetails": {
          "clusterName":"",
          "fargateDetails":{
            "issues":[],
            "managementType":""
          },
          "containerInstanceDetails":{
            "coveredContainerInstances":int,
            "compatibleContainerInstances":int
          }
        }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Solução de problemas de cobertura

Se o status da cobertura do seu cluster Amazon ECS for Insalubre, você poderá ver o motivo na coluna Problema.

A tabela a seguir fornece as etapas de solução de problemas recomendadas para problemas do Fargate (somente Amazon ECS).

Tipo de problema	Informações adicionais	Etapas para solução de problemas
Agente que não está reportando	O agente não está reportando tarefas em `TaskDefinition - '`*`TASK_DEFINITION`*`'`	Valide se a configuração do endpoint da Amazon VPC está correta.
	`VPC_ISSUE` `; for task in TaskDefinition - '` *`TASK_DEFINITION`* `'`	Veja os detalhes do problema do VPC nas informações adicionais.
O agente saiu	ExitCode: `EXIT_CODE` para tarefas em `TaskDefinition - '`*`TASK_DEFINITION`*`'`	Veja os detalhes do problema nas informações extras.
	Motivo: *`MOTIVO`* das tarefas em `TaskDefinition - '` *`TASK_DEFINITION`* `'`	
	ExitCode: `EXIT_CODE` com motivo: '*`EXIT_CODE`*' para tarefas em `TaskDefinition - '`*`TASK_DEFINITION`*`'`	
	O agente saiu: Motivo:`CannotPullContainerError :o`	A função de execução da tarefa deve ter as seguintes permissões do Amazon

Tipo de problema	Informações adicionais	Etapas para solução de problemas

	manifesto de pull image foi tentado novamente...	Elastic Container Registry (Amazon ECR):
		
		`...`
		`"ecr:GetAuthorizationToken",`
		`"ecr:BatchCheckLayerAvailability",`
		`"ecr:GetDownloadUrlForLayer",`
		`"ecr:BatchGetImage",`
		`...`
		
		Para ter mais informações, consulte Forneça permissões de ECR e detalhes da sub-rede.
		
		Depois de adicionar as permissões do Amazon ECR, você deve reiniciar a tarefa.
		
		Se o problema persistir, consulteMeu AWS Step Functions fluxo de trabalho está falhando inesperadamente.

ExitCode: `EXIT_CODE` para tarefas em `TaskDefinition - '`*`TASK_DEFINITION`*`'`	Veja os detalhes do problema nas informaçõ es extras.	
ExitCode: `EXIT_CODE` com motivo: '*`EXIT_CODE`* ' para tarefas em `TaskDefinition - '`*`TASK_DEFINITION`*`'`		

Tipo de problema	Informações adicionais	Etapas para solução de problemas
Motivo: *MOTIVO* das tarefas em `TaskDefinition - '` *TASK_DEFINITION* `'`		
Agente que não está reportando	O agente não está reportando tarefas em `TaskDefinition - '`*TASK_DEFINITION* `'`	Valide se a configuração do endpoint da Amazon VPC está correta.
	VPC_ISSUE `; for task in TaskDefinition - '` *TASK_DEFINITION* `'`	Veja os detalhes do problema do VPC nas informações adicionais.

<table>
<tr><th>Tipo de problema</th><th>Informações adicionais</th><th>Etapas para solução de problemas</th></tr>
<tr><td>Outros ou agente não provisionado</td><td>Problema não identificado, para tarefas em <code>TaskDefinition - 'TASK_DEFINITION '</code></td><td>Use as perguntas a seguir para identificar a causa raiz do problema:

<table><tr><th>Pergunta</th><th>Explicação</th></tr><tr><td>A tarefa foi iniciada antes de você ativar o Runtime Monitoring?</td><td>No Amazon ECS, as tarefas são imutáveis. Para avaliar o comportamento em tempo de execução de uma tarefa do Fargate em execução, verifique se o Runtime Monitoring já está ativado e reinicie a tarefa para adicionar o GuardDuty sidecar do contêiner.</td></tr><tr><td>A tarefa foi iniciada por um serviço sem suporte?</td><td>Atualmente, o Runtime Monitoring não oferece suporte às tarefas iniciadas por AWS Batch e. AWS CodePipeline</td></tr></table></td></tr>
</table>

Tipo de problema	Informações adicionais	Etapas para solução de problemas	
		Pergunta	Explicação
		Essa tarefa faz parte de uma implantação de serviço que começou antes de você ativar o Runtime Monitoring?	Se sim, você pode reiniciar o serviço ou atualizá-lo `forceNewDeployment` usando as etapas em Atualizar um serviço. Você também pode usar UpdateServiceou AWS CLI.
		A tarefa foi iniciada depois de excluir o cluster ECS do Runtime Monitoring?	Quando você altera a GuardDuty tag predefinida de `GuardDutyManaged` - `true` para `GuardDutyManaged` -`false`, não GuardDuty receberá os eventos de tempo de execução do cluster ECS.

Tipo de problema	Informações adicionais	Etapas para solução de problemas	
		Pergunta	Explicação
		Sua tarefa está faltando um`TaskExecutionRole` ?	É obrigatório adicionar um `TaskExecutionRole` porque GuardDuty precisa de permissões para baixar o GuardDuty contêiner do repositório ECR. Para ter mais informações, consulte Forneça permissões de ECR e detalhes da sub-rede.
		Seu serviço contém uma tarefa que tem um formato antigo de`taskArn`?	GuardDuty O Runtime Monitoring não oferece suporte à cobertura de tarefas que têm o formato antigo de`taskArn`. Para obter informações sobre Amazon Resource Names (ARNs)

Tipo de problema	Informações adicionais	Etapas para solução de problemas	
		Pergunta	Explicação
			para recursos do Amazon ECS, consulte Amazon Resource Names (ARNs) e IDs.

Cobertura para clusters Amazon EKS

Análise de estatísticas de cobertura

As estatísticas de cobertura dos clusters do EKS associados às suas próprias contas ou contas-membro são a porcentagem dos clusters do EKS saudáveis em relação a todos os clusters do EKS nas Região da AWS selecionadas. A seguinte equação representa isso como:

(Clusters íntegros/todos os clusters)*100

Selecione um dos métodos de acesso para revisar as estatísticas de cobertura de suas contas.

Console

- Faça login no AWS Management Console e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
- No painel de navegação, escolha Runtime Monitoring.
- Escolha a guia Cobertura de runtime dos clusters do EKS.
- Na guia Cobertura de runtime dos clusters do EKS, você pode visualizar as estatísticas de cobertura agregadas pelo status da cobertura que está disponível na tabela Lista de clusters.
  - Você pode filtrar a tabela Lista de clusters pelas seguintes colunas:
    - Nome do cluster
    - ID da conta
    - Tipo de gerenciamento de agentes
    - Status da cobertura

    - Versão do complemento
- Se algum dos seus clusters do EKS tiver o Status de cobertura como Não íntegro, a coluna Problema poderá incluir informações adicionais sobre o motivo do status Não íntegro.

API/CLI

- Execute a ListCoverageAPI com seu próprio ID de detector, região e ponto de extremidade de serviço válidos. É possível filtrar e classificar a lista de clusters utilizando essa API.
    - Você pode alterar o `filter-criteria` de exemplo com uma das seguintes opções para `CriterionKey`:
        - `ACCOUNT_ID`
        - `CLUSTER_NAME`
        - `RESOURCE_TYPE`
        - `COVERAGE_STATUS`
        - `ADDON_VERSION`
        - `MANAGEMENT_TYPE`
    - Você pode alterar o `AttributeName` de exemplo em `sort-criteria` com uma das seguintes opções:
        - `ACCOUNT_ID`
        - `CLUSTER_NAME`
        - `COVERAGE_STATUS`
        - `ISSUE`
        - `ADDON_VERSION`
        - `UPDATED_AT`
    - Você pode alterar *`max-results`* (até 50).
    - Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty --region us-east-1 list-coverage --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --sort-criteria '{"AttributeName":
 "EKS_CLUSTER_NAME", "OrderBy": "DESC"}' --filter-criteria
 '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID", "FilterCondition":
{"EqualsValue":"111122223333"}}] }'  --max-results 5
```

- Execute a GetCoverageStatisticsAPI para recuperar estatísticas agregadas de cobertura com base no. `statisticsType`
  - Você pode alterar o `statisticsType` de exemplo com uma das seguintes opções:
    - `COUNT_BY_COVERAGE_STATUS`: representa estatísticas de cobertura para clusters do EKS agregadas por status de cobertura.
    - `COUNT_BY_RESOURCE_TYPE`— Estatísticas de cobertura agregadas com base no tipo de AWS recurso na lista.
    - Você pode alterar o `filter-criteria` de exemplo no comando. É possível usar as seguintes opções para `CriterionKey`:
      - `ACCOUNT_ID`
      - `CLUSTER_NAME`
      - `RESOURCE_TYPE`
      - `COVERAGE_STATUS`
      - `ADDON_VERSION`
      - `MANAGEMENT_TYPE`
  - Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty --region us-east-1 get-coverage-statistics --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --statistics-type COUNT_BY_COVERAGE_STATUS
 --filter-criteria '{"FilterCriterion":[{"CriterionKey":"ACCOUNT_ID",
 "FilterCondition":{"EqualsValue":"123456789012"}}] }'
```

Se o status da cobertura do seu cluster do EKS for Não íntegro, consulte Solução de problemas de cobertura do EKS.

Configuração de notificações de alteração do status de cobertura

O status de cobertura de um cluster do EKS em sua conta pode aparecer como Não íntegro. Para detectar quando o status da cobertura se torna Não íntegro, recomendamos que você monitore o status de cobertura periodicamente e solucione o problema, se o status for Não íntegro. Como alternativa, você pode criar uma EventBridge regra da Amazon para notificá-lo quando o status da cobertura mudar de `Unhealthy` para `Healthy` ou não. Por padrão, GuardDuty publica isso no EventBridgebarramento da sua conta.

Exemplo de esquema de notificação

Em uma EventBridge regra, você pode usar os exemplos de eventos e padrões de eventos predefinidos para receber a notificação do status da cobertura. Para obter mais informações sobre a criação de uma EventBridge regra, consulte Criar regra no Guia EventBridge do usuário da Amazon.

Além disso, você pode criar um padrão de evento personalizado usando o exemplo de esquema de notificação a seguir. Substitua os valores da sua conta. Para ser notificado quando o status da cobertura do seu cluster Amazon EKS mudar de `Healthy` para`Unhealthy`, a opção `detail-type` deve ser *`GuardDuty Runtime Protection Unhealthy`*. Para ser notificado quando o status da cobertura mudar de `Unhealthy` para`Healthy`, substitua o valor de `detail-type` por *`GuardDuty Runtime Protection Healthy`*.

```
{
  "version": "0",
  "id": "event ID",
  "detail-type": "GuardDuty Runtime Protection Unhealthy",
  "source": "aws.guardduty",
  "account": "Conta da AWS ID",
  "time": "event timestamp (string)",
  "region": "Região da AWS",
  "resources": [
       ],
  "detail": {
    "schemaVersion": "1.0",
    "resourceAccountId": "string",
    "currentStatus": "string",
    "previousStatus": "string",
    "resourceDetails": {
        "resourceType": "EKS",
        "eksClusterDetails": {
            "clusterName": "string",
            "availableNodes": "string",
             "desiredNodes": "string",
             "addonVersion": "string"
         }
    },
    "issue": "string",
    "lastUpdatedAt": "timestamp"
  }
}
```

Solução de problemas de cobertura do EKS

Se o status da cobertura do seu cluster EKS for`Unhealthy`, você poderá visualizar o erro correspondente na coluna Problema no GuardDuty console ou usando o tipo de CoverageResourcedados.

Ao trabalhar com tags de inclusão ou exclusão para monitorar seus clusters do EKS seletivamente, pode levar algum tempo para que as tags sejam sincronizadas. Isso pode afetar o status de cobertura do cluster do EKS associado. É possível tentar remover e adicionar a tag correspondente (inclusão ou exclusão) novamente. Para obter mais informações, consulte Marcar os recursos do Amazon EKS no Guia do desenvolvedor do Amazon EKS.

A estrutura de um problema de cobertura é `Issue type:Extra information`. Normalmente, os problemas terão Informações adicionais opcionais que poderão incluir uma exceção específica do lado do cliente ou uma descrição sobre o problema. Com base em informações adicionais, as tabelas a seguir fornecem as etapas recomendadas para solucionar os problemas de cobertura de seus clusters EKS.

Tipo de problema (prefixo)	Informações adicionais	Etapas para solução de problemas
Falha na criação de complemento	O complemento não `aws-guardduty-agent` é compatível com a versão atual do cluster *`ClusterName`* . O complemento especificado é compatível.	Certifique-se de usar uma dessas versões do Kubernetes compatíveis com a implantação do complemento EKS `aws-guardduty-agent` . Para ter mais informações, consulte Versões do Kubernetes suportadas pelo agente de segurança GuardDuty . Para obter informações sobre como atualizar sua versão do Kubernetes, consulte Atualizar uma versão do

Tipo de problema (prefixo)	Informações adicionais	Etapas para solução de problemas
		Kubernetes do cluster do Amazon EKS.
Falha na criação de complemento Falha na atualização do complemento Status do complemento não íntegro	Problema no complemento do EKS - `AddonIssueCode : AddonIssueMessage`	Para obter informações sobre as etapas recomendadas para um código de problema específico do complemento, consulte Troubleshooting steps for Addon creation/updatation error with Addon issue code. Para obter uma lista dos códigos de problemas adicionais que você pode enfrentar nesse problema, consulte AddonIssue.
Falha na criação de endpoint da VPC	*A criação de endpoints de VPC não é compatível com VPCid de VPC compartilhada*	O Runtime Monitoring agora oferece suporte ao uso de uma VPC compartilhada em uma organização. Certifique-se de que suas contas atendam a todos os pré-requisitos. Para ter mais informações, consulte Pré-requisitos para usar a VPC compartilhada.

Tipo de problema (prefixo)	Informações adicionais	Etapas para solução de problemas
	Somente ao usar VPC compartilhada com configuração automatizada de agentes ID da conta do proprietário *111122223333* para VPC compartilhada O vPCid não tem o *Runtime Monitoring, a configuração automatizada* do agente ou ambos ativados.	A conta compartilhada do proprietário da VPC deve habilitar o Runtime Monitoring e a configuração automática do agente para pelo menos um tipo de recurso (Amazon EKS ou Amazon ECS ())AWS Fargate. Para ter mais informações, consulte Pré-requisitos específicos para o monitoramento de tempo de execução GuardDuty.

Tipo de problema (prefixo)	Informações adicionais	Etapas para solução de problemas
	A habilitação do DNS privado requer os atributos da VPC enableDnsSupport e enableDnsHostnames definidos como true para vpcId (Serviço: Ec2, Código de status: 400, ID da solicitação: a1b2c3d4-5678-90ab-cdef-EXAMPLE11111).	Verifique se os seguintes atributos da VPC estão definidos como `true`: `enableDnsSupport` e `enableDnsHostnames` . Para obter mais informações, consulte Atributos de DNS na sua VPC. Se você estiver usando o console da Amazon VPC em https://console.aws.amazon.com/vpc/ para criar a Amazon VPC, certifique-se de selecionar Habilitar nomes de host DNS e Habilitar resolução de DNS. Para obter mais informações, consulte Opções de configuração da VPC.

Tipo de problema (prefixo)	Informações adicionais	Etapas para solução de problemas
Falha na exclusão do endpoint VPC compartilhado	*A exclusão compartilhada do VPC endpoint não é permitida para a ID da conta 111122223333 , VPC compartilhada VPCid, ID da conta do proprietário 555555555555.*	Etapas potenciais: • A desativação do status do Runtime Monitoring da conta compartilhada do participante da VPC não afeta a política de endpoint da VPC compartilhada e o grupo de segurança que existe na conta do proprietário. Para excluir o endpoint e o grupo de segurança da VPC compartilhados, você deve desativar o Runtime Monitoring ou o status de configuração automática do agente na conta compartilhada do proprietário da VPC. • A conta compartilhada do participante da VPC não pode excluir o endpoint e o grupo de segurança da VPC compartilhados hospedados na conta compartilhada do proprietário da VPC.

Tipo de problema (prefixo)	Informações adicionais	Etapas para solução de problemas
Clusters locais do EKS	Os complementos do EKS não são compatíveis com clusters de Outposts locais.	Não acionável. Para obter mais informações, consulte Amazon EKS em AWS Outposts.
A permissão de habilitação do Monitoramento de runtime do EKS não foi concedida	(pode ou não mostrar informações adicionais)	1. Se houver informaçõ es adicionais disponíve is para esse problema, corrija a causa raiz e siga a próxima etapa. 2. Desative o Monitoram ento de runtime do EKS e depois ative-o novamente. Certifique-se de que o GuardDuty agente também seja implantado, seja de forma automática GuardDuty ou manual.

Tipo de problema (prefixo)	Informações adicionais	Etapas para solução de problemas
Provisionamento de recursos de habilitação do Monitoramento de runtime do EKS em andamento	(pode ou não mostrar informações adicionais)	Não acionável. Depois de habilitar o Monitoramento de runtime do EKS, o status da cobertura pode permanecer `Unhealthy` até que a etapa de provisionamento de recursos seja concluída. O status da cobertura é monitorado e atualizado periodicamente.
Outros (qualquer outro problema)	Erro devido à falha na autorização	Desative o Monitoramento de runtime do EKS e depois ative-o novamente. Certifique-se de que o GuardDuty agente também seja implantado, de forma automática GuardDuty ou manual.

Erro na criação ou atualização do complemento	Etapas de solução de problemas
Problema do complemento EKS - `InsufficientNumberOfReplicas` : O complemento não está íntegro porque não tem o número desejado de réplicas.	Usando a mensagem do problema, você pode identificar e corrigir a causa raiz. Você pode começar descrevendo seu cluster. Por exemplo, use `kubectl describe pods` para identificar a causa raiz da falha do pod.

Erro na criação ou atualização do complemento	Etapas de solução de problemas
	Depois de corrigir a causa raiz, repita a etapa (criação ou atualização do complemento).
Problema do complemento EKS -`Admission RequestDenied` : o webhook de admissão `"validate.kyverno.svc-fail"` negou a solicitação: política de violação `DaemonSet/amazon-guardduty/aws-guardduty-agent` de recursos:: restrict-image-registries:`autogen-validate-registries` ...	1. O cluster Amazon EKS ou o administrador de segurança devem revisar a política de segurança que está bloqueando a atualização do complemento. 2. Você deve desativar o controlador (webhook) ou fazer com que o controlador aceite as solicitações do Amazon EKS.
Problema do complemento EKS -`ConfigurationConflict` : Conflitos encontrados ao tentar se inscrever. Não continuará devido ao modo de resolução de conflitos. `Conflicts: DaemonSet.apps aws-guardduty-agent - .spec.template.spec.containers[name="aws-guardduty-agent"].image`	Ao criar ou atualizar o complemento, forneça o sinalizador de `OVERWRITE` resolução de conflitos. Isso potencialmente substituirá todas as alterações feitas diretamente nos recursos relacionados no Kubernetes usando a API do Kubernetes. Você pode primeiro excluir o complemento e depois reinstalá-lo.

Erro na criação ou atualização do complemento	Etapas de solução de problemas

Problema do complemento EKS - `AccessDenied: priorityclasses.scheduling.k8s.io "aws-guardduty-agent.priorityclass" is forbidden: User "eks:addon-manager" cannot patch resource "priorityclasses" in API group "scheduling.k8s.io" at the cluster scope`	Você deve adicionar `eks:addon-cluster-admin ClusterRoleBinding` manualmente a permissão ausente ao. Adicione o seguinte `yaml` a`eks:addon-cluster-admin` :
	`---`
	`kind: ClusterRoleBinding`
	`apiVersion: rbac.authorization.k8s.io/v1`
	`metadata:`
	`  name: eks:addon-cluster-admin`
	`subjects:`
	`- kind: User`
	`  name: eks:addon-manager`
	`  apiGroup: rbac.authorization.k8s.io`
	`roleRef:`
	`  kind: ClusterRole`
	`  name: cluster-admin`
	`  apiGroup: rbac.authorization.k8s.io`
	`---`
	Agora você pode aplicar isso `yaml` ao seu cluster Amazon EKS usando o seguinte comando:
	`kubectl apply -f eks-addon-cluster-admin.yaml`

Erro na criação ou atualização do complemento	Etapas de solução de problemas
Problema do complemento EKS - `AccessDenied: admission webhook "validation.gatekeeper.sh" denied the request: [all-namespace-must-have-label-owner] All namespaces must have an `owner` label`	Você deve desativar o controlador ou fazer com que ele aceite as solicitações do cluster Amazon EKS. Antes de criar ou atualizar o complemento, você também pode criar um GuardDuty namespace e rotulá-lo como. `owner`

Perguntas frequentes (FAQs)

Conteúdo

Por que o status da cobertura do meu recurso é **`Unhealthy`** mesmo depois de ativar o Runtime Monitoring, implantar o agente de GuardDuty segurança e atender a todos os pré-requisitos?

Se você acabou de implantar o agente de GuardDuty segurança (por meio da configuração automática do agente ou manualmente) ou seguiu as etapas recomendadas para solucionar um problema de cobertura, pode levar alguns minutos para que o status da cobertura fique íntegro. Você pode verificar o status da cobertura periodicamente ou configurar a Amazon EventBridge (EventBridge) para receber uma notificação quando o status da cobertura mudar.

Quem pode ver o status da cobertura em tempo de execução de um recurso que pertence ao meu Conta da AWS?

Como conta de membro ou conta independente, você pode visualizar as estatísticas de cobertura dos recursos associados às suas próprias contas. Como conta de GuardDuty administrador

delegado de uma organização, você pode visualizar as estatísticas de cobertura dos recursos associados à sua conta e das contas dos membros que pertencem à sua organização.

Configurar o monitoramento da CPU e da memória

Depois de ativar o Runtime Monitoring e avaliar se o status da cobertura do seu cluster é íntegro, você pode configurar e visualizar as métricas do insight.

Os tópicos a seguir podem ajudá-lo a avaliar o desempenho do agente implantado em relação aos limites de CPU e memória do GuardDuty agente.

Configurando o monitoramento no cluster Amazon ECS

As etapas a seguir do Guia CloudWatch do usuário da Amazon podem ajudá-lo a avaliar o desempenho do agente implantado em relação aos limites de CPU e memória do GuardDuty agente:

1. Configuração do Container Insights no Amazon ECS para métricas de nível de cluster e serviço
2. Métricas do Amazon ECS Container Insights

Configurando o monitoramento no cluster Amazon EKS

Depois que o agente de GuardDuty segurança for implantado e você avaliar se o status da cobertura do seu cluster está íntegro, você pode configurar e visualizar as métricas do Container Insight.

Avalie o desempenho do agente de segurança

1. Configuração do Container Insights no Amazon EKS e no Kubernetes no Guia do usuário da Amazon CloudWatch
2. Métricas do Amazon EKS e do Kubernetes Container Insights no Guia do usuário da Amazon CloudWatch

Gerencie o desempenho com o agente de segurança v1.5.0 e superior

Com o Security Agent v1.5.0 e versões posteriores, quando os insights indicam que o GuardDuty agente associado está atingindo os limites atribuídos, você pode configurar parâmetros específicos. Para ter mais informações, consulte Configurar os parâmetros do complemento EKS.

Tipos de eventos de tempo de execução coletados que GuardDuty usam

O agente GuardDuty de segurança coleta os seguintes tipos de eventos e os envia ao GuardDuty back-end para detecção e análise de ameaças. GuardDuty não torna esses eventos acessíveis para você. Se GuardDuty detectar uma ameaça potencial e gerar uma descoberta do Runtime Monitoring, você poderá visualizar os detalhes da descoberta correspondente. Para obter mais informações sobre como GuardDuty usa os tipos de eventos coletados, consulteOptar por não usar seus dados para melhorar o serviço.

Eventos do processo

Nome do campo	Descrição
Nome do processo	Nome do processo observado.
Caminho do processo	Caminho absoluto do processo executável.
ID do processo	O ID atribuído ao processo pelo sistema operacional.
PID do namespace	O ID do processo em um namespace de PID secundário diferente do namespace de PID no nível do host. Para processos em um contêiner , é o ID do processo observado dentro do contêiner.
ID do usuário do processo	O ID exclusivo do usuário que executou o processo.
UUID do processo	A ID exclusiva atribuída ao processo por GuardDuty.
GID do processo	ID de processo do grupo de processos.
EGID do processo	ID de grupo efetivo do grupo de processos.
EUID do processo	ID de usuário efetivo do processo.

Nome do campo	Descrição
Nome de usuário do processo	O nome do usuário que executou o processo.
Hora de início do processo	A hora de criação do processo. Esse campo está no formato de string de data UTC (`2023-03-22T19:37:20.168Z`).
Processar SHA-256 do executável	O hash `SHA256` do executável do processo.
Caminho do script de processo	Caminho do arquivo de script que foi executado .
Variável de ambiente do processo	A variável de ambiente disponibilizada para o processo. Somente `LD_PRELOAD` e `LD_LIBRARY_PATH` são coletados.
Present Working Directory (PWD – Diretório de trabalho presente) do processo	Diretório de trabalho presente do processo.
Processo pai	Detalhes do processo pai. Um processo pai é um processo que criou o processo observado.
Argumentos da linha de comando Atualmente, esse campo está limitado às versões específicas do agente correspon dentes ao tipo de recurso: • Fargate (somente Amazon ECS) com agente de GuardDuty segurança v1.0.0 e superior. • Instâncias do Amazon EC2 com agente de GuardDuty segurança v1.0.0 e superior. • Clusters Amazon EKS com agente de segurança v1.4.0 e superior. Para ter mais informações, consulte GuardDuty histórico de lançamento do agente.	Argumentos de linha de comando fornecidos no momento da execução do processo. Esse campo pode conter dados confidenciais do cliente.

Eventos de contêineres

Nome do campo	Descrição
Nome do contêiner	O nome do contêiner. Quando disponível, esse campo exibe o valor do rótulo `io.kubenetes.container.name` .
UID do contêiner	O ID exclusivo do contêiner atribuído pelo runtime do contêiner.
Runtime do contêiner	O runtime do contêiner (como `docker` ou `containerd`) usado para executar o contêiner.
ID da imagem do contêiner	O ID da imagem do contêiner.
Nome da imagem do contêiner	O nome da imagem do contêiner.

AWS Fargate Eventos de tarefas (somente Amazon ECS)

Nome do campo	Descrição
Nome do recurso Amazon da tarefa (ARN)	O ARN da tarefa.
Nome do cluster	O nome do cluster Amazon ECS.
Nome de família	O sobrenome da definição da tarefa. O `family` é usado como um nome para a definição da tarefa usada para iniciar a tarefa.
Nome do serviço	O nome do serviço Amazon ECS, se a tarefa foi iniciada como parte de um serviço.
Tipo de execução	A infraestrutura na qual sua tarefa é executada. Para o Runtime Monitoring com o tipo de recurso como`ECSCluster` , o tipo de lançamento pode ser `EC2` ou`FARGATE`.

Nome do campo	Descrição
CPU	O número de unidades de CPU usadas pela tarefa, conforme expresso na definição da tarefa.

Eventos de pod do Kubernetes

Nome do campo	Descrição
ID do pod	O ID do pod do Kubernetes.
Nome do pod	Nome do pod do Kubernetes.
Namespace do pod	Nome do namespace do Kubernetes ao qual a workload do Kubernetes pertence.
Nome do cluster do Kubernetes	Nome do cluster do Kubernetes.

Eventos de DNS

Nome do campo	Descrição
Tipo de soquete	Tipo de soquete para indicar a semântica de comunicação. Por exemplo, `SOCK_RAW`.
Família de endereços	Representa o protocolo de comunicação associado ao endereço. Por exemplo, a família de endereços `AF_INET` é usada para o protocolo IPv4.
ID de direção	O ID de direção da conexão.
Número do protocolo	O número do protocolo da camada 4, como 17 para UDP e 6 para TCP.
IP de endpoint remoto de DNS	O IP remoto da conexão.

Nome do campo	Descrição
Porta de endpoint remoto de DNS	O número da porta da conexão.
IP do endpoint local de DNS	O IP local da conexão.
Porta do endpoint local de DNS	O número da porta da conexão.
Carga útil de DNS	A carga útil dos pacotes DNS que contém consultas e respostas de DNS.

Eventos abertos

Nome do campo	Descrição
Caminho de arquivo	Caminho de arquivo que é aberto nesse evento.
Sinalizadores	Descreve o modo de acesso ao arquivo, como somente de leitura, somente de gravação e de leitura-gravação.

Evento do módulo de carga

Nome do campo	Descrição
Nome do módulo	Nome do módulo carregado no kernel.

Eventos do Mprotect

Nome do campo	Descrição
Intervalo de endereços	O intervalo de endereços para o qual as proteções de acesso foram modificadas.

Nome do campo	Descrição
Regiões da memória	Especifica a região do espaço de endereços de um processo, como pilha e heap.
Sinalizadores	Representa as opções que controlam o comportamento desse evento.

Eventos de montagem

Nome do campo	Descrição
Destino de montagem	O caminho em que a origem de montagem está montada.
Fonte de montagem	O caminho no host que está montado no destino de montagem.
Tipo do sistema de arquivos	Representa o tipo de sistema de arquivos montado.
Sinalizadores	Representa as opções que controlam o comportamento desse evento.

Eventos de links

Nome do campo	Descrição
Caminho do link	O caminho em que o link físico é criado.
Caminho de destino	O caminho do arquivo para o qual o link físico aponta.

Eventos do Symlink

Nome do campo	Descrição
Caminho do link	Caminho em que o link simbólico é criado.

Nome do campo	Descrição
Caminho de destino	Caminho do arquivo para o qual o link simbólico aponta.

Eventos Dup

Nome do campo	Descrição
Antigo descritor de arquivo	Um descritor de arquivo que representa um objeto de arquivo aberto.
Novo descritor de arquivo	Um novo descritor de arquivo que é uma duplicata do antigo descritor de arquivo. Os antigos e novos descritores de arquivo representam o mesmo objeto de arquivo aberto.
IP de endpoint remoto de Dup	O endereço IP remoto do soquete de rede representado pelo antigo descritor de arquivo. Aplicável somente quando o antigo descritor de arquivo representa um soquete de rede.
Porta de endpoint remoto de Dup	A porta remota do soquete de rede representado pelo antigo descritor de arquivo. Aplicável somente quando o antigo descritor de arquivo representa um soquete de rede.
IP do endpoint local de Dup	O endereço IP local do soquete de rede representado pelo antigo descritor de arquivo. Aplicável somente quando o antigo descritor de arquivo representa um soquete de rede.
Porta do endpoint local de Dup	A porta local do soquete de rede representado pelo antigo descritor de arquivo. Aplicável somente quando o antigo descritor de arquivo representa um soquete de rede.

Evento do mapa de memória

Nome do campo	Descrição
Caminho de arquivo	Caminho de arquivo para o qual a memória está mapeada.

Eventos de soquete

Nome do campo	Descrição
Família de endereços	Representa o protocolo de comunicação associado ao endereço. Por exemplo, a família de endereços `AF_INET` é usada para o protocolo IPv4.
Tipo de soquete	Tipo de soquete para indicar a semântica de comunicação. Por exemplo, `SOCK_RAW`.
Número do protocolo	Especifica um protocolo específico dentro da família de endereços. Geralmente, há um único protocolo nas famílias de endereços. Por exemplo, a família de endereços `AF_INET` só tem o protocolo IP.

Eventos de conexão

Nome do campo	Descrição
Família de endereços	Representa o protocolo de comunicação associado ao endereço. Por exemplo, a família de endereços `AF_INET` é usada para o protocolo IPv4.
Tipo de soquete	Tipo de soquete para indicar a semântica de comunicação. Por exemplo, `SOCK_RAW`.
Número do protocolo	Especifica um protocolo específico dentro da família de endereços. Geralmente, há um único protocolo nas famílias de endereços. Por exemplo, a família de endereços `AF_INET` só tem o protocolo IP.
Caminho de arquivo	Caminho do arquivo de soquete se a família de endereços for `AF_UNIX`.
IP de endpoint remoto	O IP remoto da conexão.

Nome do campo	Descrição
Porta de endpoint remoto	O número da porta da conexão.
IP do endpoint local	O IP local da conexão.
Porta do endpoint local	O número da porta da conexão.

Processar eventos Readv da VM

Nome do campo	Descrição
Sinalizadores	Representa as opções que controlam o comportamento desse evento.
PID de destino	ID de processo do qual a memória está sendo lida.
UUID do processo de destino	O ID exclusivo do processo de destino.
Caminho executável de destino	Caminho absoluto do arquivo executável do processo de destino.

Processar eventos Writev da VM

Nome do campo	Descrição
Sinalizadores	Representa as opções que controlam o comportamento desse evento.
PID de destino	ID de processo no qual a memória está sendo gravada.
UUID do processo de destino	O ID exclusivo do processo de destino.
Caminho executável de destino	Caminho absoluto do arquivo executável do processo de destino.

Eventos Ptrace

Nome do campo	Descrição
PID de destino	ID de processo do processo de destino.
UUID do processo de destino	O ID exclusivo do processo de destino.
Caminho executável de destino	Caminho absoluto do arquivo executável do processo de destino.
Sinalizadores	Representa as opções que controlam o comportamento desse evento.

Vincular eventos

Nome do campo	Descrição
Família de endereços	Representa o protocolo de comunicação associado ao endereço. Por exemplo, a família de endereços `AF_INET` é usada para o protocolo IPv4.
Tipo de soquete	Tipo de soquete para indicar a semântica de comunicação. Por exemplo, `SOCK_RAW`.
Número do protocolo	O número do protocolo da camada 4, como 17 para UDP e 6 para TCP.
IP do endpoint local	O IP local da conexão.
Porta de endpoint local	O número da porta da conexão.

Ouça os eventos

Nome do campo	Descrição
Família de endereços	Representa o protocolo de comunicação associado ao endereço. Por exemplo, a família de endereços `AF_INET` é usada para o protocolo IPv4.
Tipo de soquete	Tipo de soquete para indicar a semântica de comunicação. Por exemplo, `SOCK_RAW`.
Número do protocolo	O número do protocolo da camada 4, como 17 para UDP e 6 para TCP.
IP do endpoint local	O IP local da conexão.
Porta de endpoint local	O número da porta da conexão.

Renomear eventos

Nome do campo	Descrição
Caminho de arquivo	Caminho onde está o arquivo que foi renomeado.
Destino	O novo caminho do arquivo.

Definir eventos de UID

Nome do campo	Descrição
Novo EUID	O novo ID de usuário efetivo do processo.
Novo UID	O novo ID de usuário do processo.

Eventos Chmod

Nome do campo	Descrição
Caminho de arquivo	Caminho do arquivo que invoca esse evento.
Modo de arquivo	As permissões de acesso atualizadas para o arquivo associado.

Agente de hospedagem de repositórios Amazon ECR GuardDuty

As seções a seguir listam os repositórios do Amazon Elastic Container Registry (Amazon ECR) GuardDuty onde hospeda o agente de segurança que é implantado em seus clusters Amazon EKS e Amazon ECS.

Conteúdo

Repositório para GuardDuty agente em clusters Amazon EKS

A tabela a seguir mostra os repositórios do Amazon ECR que hospedam o agente complementar do Amazon EKS para GuardDuty (`aws-guardduty-agent`) para cada um. Região da AWS

Região da AWS	URI do repositório do Amazon ECR
Oeste dos EUA (Oregon)	`039403964562.dkr.ecr.us-west-2.amazonaws.com`
Europa (Paris)	`113643092156.dkr.ecr.eu-west-3.amazonaws.com`
Ásia-Pacífico (Mumbai)	`610108029387.dkr.ecr.ap-south-1.amazonaws.com`
Ásia-Pacífico (Hyderabad)	`618745550137.dkr.ecr.ap-south-2.amazonaws.com`
Canadá (Central)	`001188825231.dkr.ecr.ca-central-1.amazonaws.com`

Região da AWS	URI do repositório do Amazon ECR
Oriente Médio (Emirados Árabes Unidos)	601769779514.dkr.ecr.me-central-1.amazonaws.com
Europa (Londres)	109118265657.dkr.ecr.eu-west-2.amazonaws.com
Europa (Irlanda)	373421517865.dkr.ecr.us-west-1.amazonaws.com
Leste dos EUA (N. da Virgínia)	031903291036.dkr.ecr.us-east-1.amazonaws.com
Leste dos EUA (Ohio)	591382732059.dkr.ecr.us-east-2.amazonaws.com
Europa (Irlanda)	673884943994.dkr.ecr.eu-west-1.amazonaws.com
América do Sul (São Paulo)	941219317354.dkr.ecr.sa-east-1.amazonaws.com
Europa (Estocolmo)	366771026645.dkr.ecr.eu-north-1.amazonaws.com
Europa (Frankfurt)	409493279830.dkr.ecr.eu-central-1.amazonaws.com
Europa (Zurique)	718440343717.dkr.ecr.eu-central-2.amazonaws.com
Ásia-Pacífico (Singapura)	584580519942.dkr.ecr.ap-southeast-1.amazonaws.com
Ásia-Pacífico (Sydney)	011662287384.dkr.ecr.ap-southeast-2.amazonaws.com
Ásia-Pacífico (Jacarta)	617474730032.dkr.ecr.ap-southeast-3.amazonaws.com

Região da AWS	URI do repositório do Amazon ECR
Ásia-Pacífico (Tóquio)	781592569369.dkr.ecr.ap-northeast-1.amazonaws.com
Ásia-Pacífico (Seul)	732248494576.dkr.ecr.ap-northeast-2.amazonaws.com
Asia Pacific (Osaka)	810724417379.dkr.ecr.ap-northeast-3.amazonaws.com
Ásia-Pacífico (Hong Kong)	790429075973.dkr.ecr.ap-east-1.amazonaws.com
Oriente Médio (Barém)	541829937850.dkr.ecr.me-south-1.amazonaws.com
Europa (Milão)	528450769569.dkr.ecr.eu-south-1.amazonaws.com
Europa (Espanha)	531047660167.dkr.ecr.eu-south-2.amazonaws.com
África (Cidade do Cabo)	379032919888.dkr.ecr.af-south-1.amazonaws.com
Ásia-Pacífico (Melbourne)	750462861327.dkr.ecr.ap-southeast-4.amazonaws.com
Israel (Tel Aviv)	292660727137.dkr.ecr.il-central-1.amazonaws.com

Repositório para GuardDuty agente em AWS Fargate (somente Amazon ECS)

A tabela a seguir mostra os repositórios do Amazon ECR que hospedam o GuardDuty agente (somente AWS Fargate Amazon ECS) para cada um. Região da AWS

Região da AWS	URI do repositório do Amazon ECR
Oeste dos EUA (Oregon)	`733349766148.dkr.ecr.us-west-2.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Paris)	`665651866788.dkr.ecr.eu-west-3.amazonaws.com/aws-guardduty-agent-fargate`
Ásia-Pacífico (Mumbai)	`251508486986.dkr.ecr.ap-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Ásia-Pacífico (Hyderabad)	`950823858135.dkr.ecr.ap-south-2.amazonaws.com/aws-guardduty-agent-fargate`
Canadá (Central)	`354763396469.dkr.ecr.ca-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Oriente Médio (Emirados Árabes Unidos)	`000014521398.dkr.ecr.me-central-1.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Londres)	`892757235363.dkr.ecr.eu-west-2.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Irlanda)	`684579721401.dkr.ecr.us-west-1.amazonaws.com/aws-guardduty-agent-fargate`
Leste dos EUA (N. da Virgínia)	`593207742271.dkr.ecr.us-east-1.amazonaws.com/aws-guardduty-agent-fargate`
Leste dos EUA (Ohio)	`307168627858.dkr.ecr.us-east-2.amazonaws.com/aws-guardduty-agent-fargate`
Europa (Irlanda)	`694911143906.dkr.ecr.eu-west-1.amazonaws.com/aws-guardduty-agent-fargate`
América do Sul (São Paulo)	`758426053663.dkr.ecr.sa-east-1.amazonaws.com/aws-guardduty-agent-fargate`

Região da AWS	URI do repositório do Amazon ECR
Europa (Estocolmo)	591436053604.dkr.ecr.eu-north-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Frankfurt)	323658145986.dkr.ecr.eu-central-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Zurique)	529164026651.dkr.ecr.eu-central-2.amazonaws.com/aws-guardduty-agent-fargate
Ásia-Pacífico (Singapura)	174946120834.dkr.ecr.ap-southeast-1.amazonaws.com/aws-guardduty-agent-fargate
Ásia-Pacífico (Sydney)	005257825471.dkr.ecr.ap-southeast-2.amazonaws.com/aws-guardduty-agent-fargate
Ásia-Pacífico (Jacarta)	510637619217.dkr.ecr.ap-southeast-3.amazonaws.com/aws-guardduty-agent-fargate
Ásia-Pacífico (Tóquio)	533107202818.dkr.ecr.ap-northeast-1.amazonaws.com/aws-guardduty-agent-fargate
Ásia-Pacífico (Seul)	914738172881.dkr.ecr.ap-northeast-2.amazonaws.com/aws-guardduty-agent-fargate
Asia Pacific (Osaka)	273192626886.dkr.ecr.ap-northeast-3.amazonaws.com/aws-guardduty-agent-fargate
Ásia-Pacífico (Hong Kong)	258348409381.dkr.ecr.ap-east-1.amazonaws.com/aws-guardduty-agent-fargate
Oriente Médio (Barém)	536382113932.dkr.ecr.me-south-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Milão)	266869475730.dkr.ecr.eu-south-1.amazonaws.com/aws-guardduty-agent-fargate
Europa (Espanha)	919611009337.dkr.ecr.eu-south-2.amazonaws.com/aws-guardduty-agent-fargate

Região da AWS	URI do repositório do Amazon ECR
África (Cidade do Cabo)	`197869348890.dkr.ecr.af-south-1.amazonaws.com/aws-guardduty-agent-fargate`
Ásia-Pacífico (Melbourne)	`251357961535.dkr.ecr.ap-southeast-4.amazonaws.com/aws-guardduty-agent-fargate`
Israel (Tel Aviv)	`870907303882.dkr.ecr.il-central-1.amazonaws.com/aws-guardduty-agent-fargate`

GuardDuty histórico de lançamento do agente

As seções a seguir fornecem a versão de lançamento para o GuardDuty agente que é implantado em instâncias do Amazon EC2, clusters do Amazon ECS e clusters do Amazon EKS.

GuardDuty agente de segurança para instâncias do Amazon EC2

Versão do agente	Notas de release	Data de disponibilidade
v1.1.0	Oferece suporte à configuração GuardDuty automatizada de agentes no Runtime Monitoring para instâncias do Amazon EC2. Suporta novos sinais e descobertas de segurança lançados com o anúncio da disponibilidade geral do Runtime Monitoring para instâncias do EC2. Melhoria geral do desempenho.	26 de março de 2024

Versão do agente	Notas de release	Data de disponibilidade
v1.0.2	Compatível com as AMIs mais recentes do Amazon ECS.	2 de fevereiro de 2022
v1.0.1	Ajustes e aprimoramentos gerais de desempenho As versões do agente lançadas antes da v1.0.2 são incompatíveis com as AMIs do Amazon ECS lançadas após 31 de janeiro de 2024.	23 de janeiro de 2024
v1.0.0	Versão inicial da instalação do RPM. As versões do agente lançadas antes da v1.0.2 são incompatíveis com as AMIs do Amazon ECS lançadas após 31 de janeiro de 2024.	26 de novembro de 2023

A chave pública, a assinatura de x86_64 RPM, a assinatura de arm64 RPM e o link de acesso correspondente aos scripts de RPM hospedados nos buckets do Amazon S3 podem ser formados a partir dos seguintes modelos. Substitua o valor do Região da AWS ID da AWS conta e a versão do GuardDuty agente para acessar os scripts de RPM. Os modelos a seguir incluem a versão mais recente do agente para instâncias do Amazon EC2.

- Chave pública:

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/publickey.pem
```

- GuardDuty assinatura RPM do agente de segurança:

  Assinatura de x86_64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/amazon-guardduty-agent-1.1.0.x86_64.sig
```

Assinatura do arm64 RPM

```
s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/amazon-guardduty-agent-1.1.0.arm64.sig
```

- Acesse os links para os scripts de RPM no bucket do Amazon S3:

  Link de acesso para x86_64 RPM

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/x86_64/amazon-guardduty-agent-1.1.0.x86_64.rpm
  ```

  Link de acesso para arm64 RPM

  ```
  s3://694911143906-eu-west-1-guardduty-agent-rpm-artifacts/1.1.0/arm64/amazon-guardduty-agent-1.1.0.arm64.rpm
  ```

Região da AWS	Nome da região	AWS ID da conta
eu-west-1	Europa (Irlanda)	694911143906
us-east-1	Leste dos EUA (Norte da Virgínia)	593207742271
us-east-2	Leste dos EUA (Ohio)	733349766148
eu-west-3	Europa (Paris)	665651866788
us-east-2	Leste dos EUA (Ohio)	307168627858
eu-central-1	Europa (Frankfurt)	323658145986
ap-northeast-2	Ásia-Pacífico (Seul)	914738172881
eu-north-1	Europa (Estocolmo)	591436053604
ap-east-1	Ásia-Pacífico (Hong Kong)	258348409381
me-south-1	Oriente Médio (Barém)	536382113932

eu-west-2	Europa (Londres)	892757235363
ap-northeast-1	Ásia-Pacífico (Tóquio)	533107202818
ap-southeast-1	Ásia-Pacífico (Singapura)	174946120834
ap-south-1	Ásia-Pacífico (Mumbai)	251508486986
ap-southeast-3	Ásia-Pacífico (Jacarta)	510637619217
sa-east-1	América do Sul (São Paulo)	758426053663
ap-northeast-3	Asia Pacific (Osaka)	273192626886
eu-south-1	Europa (Milão)	266869475730
af-south-1	África (Cidade do Cabo)	197869348890
ap-southeast-2	Ásia-Pacífico (Sydney)	00:5257.825.471
me-central-1	Oriente Médio (Emirados Árabes Unidos)	00:00:1452.1398
us-west-1	Oeste dos EUA (N. da Califórnia)	684579721401
ca-central-1	Canadá (Central)	354763396469
ap-south-2	Ásia-Pacífico (Hyderabad)	950823858135
eu-south-2	Europa (Espanha)	919611009337
eu-central-2	Europa (Zurique)	529164026651
ap-southeast-4	Ásia-Pacífico (Melbourne)	251357961535
il-central-1	Israel (Tel Aviv)	870907303882

GuardDuty agente de segurança para AWS Fargate (somente Amazon ECS)

A tabela a seguir mostra o histórico de versões do agente de GuardDuty segurança do Fargate (somente Amazon ECS).

Versão do agente	Imagem de contêiner	Notas de release	Data de disponibilidade
v1.0.0	x86_64 (AMD64): `sha256:359b8b014e5076c625daa1056090e522631587a7afa3b2e055edda6bd1141017` Graviton (ARM64): `sha256:b9438690fa8a86067180a11658bec0f4f838ae3fbd225d04b9306250648b3984`	Lançamento inicial do agente de GuardDuty segurança para AWS Fargate (somente Amazon ECS).	26 de novembro de 2023

GuardDuty agente de segurança para clusters Amazon EKS

A tabela a seguir mostra o histórico de versões do GuardDuty agente complementar Amazon EKS.

Versão do agente	Imagem de contêiner	Notas de release	Data de disponibilidade	Fim do suporte padrão [1]
v1.5.0	x86_64 (AMD64): `sha256:66d491927763742660faa87cc2c39bb97b7873039157ae8b90bc999cb73d0b9c` Graviton (ARM64): `sha256:537a330b2dd82357024fb6daeb876`	• Ajustes e aprimoramentos gerais de desempenho. • Aprimoramentos de	07 de março de 2024	–

Versão do agente	Imagem de contêiner	Notas de release	Data de disponibilidade	Fim do suporte padrão [1]
	1034b7defd43b10dffe0792c9e6d0778b40	segurança, incluindo novos tipos de eventos em. Tipos de eventos de runtime coletados • Aprimoramentos de desempenho em relação ao uso da CPU.		
v1.4.1	x86_64 (AMD64): sha256:66d491927763742660faa87cc2c39bb97b7873039157ae8b90bc999cb73d0b9c Graviton (ARM64): sha256:537a330b2dd82357024fb6daeb8761034b7defd43b10dffe0792c9e6d0778b40	Ajustes e aprimoramentos gerais de desempenho.	16 de janeiro de 2024	–

Versão do agente	Imagem de contêiner	Notas de release	Data de disponibilidade	Fim do suporte padrão [1]
v1.4.0	x86_64 (AMD64): `sha256:848ce13d9430bad554ac23d4699551505326ada2a88e1a721fe9f86b56b52c0f` Graviton (ARM64): `sha256:0c650aeafeeb5f2bcb8b989ac849bedc1fae1a4de1cf6306ffdd9c6aebe67f8e`	O ponto de montagem do manifesto suporta uma melhor coleta de dados AppArmor configuração no manifesto Colete o argumento da linha de comando Ajustes e aprimoramentos gerais de desempenho	21 de dezembro de 2023	–
v1.3.1	x86_64 (AMD64): `sha256:55578fcb7b73097ade5c8404390ef16cf76a7b568490abaae01ac75992b3ea29` Graviton (ARM64): `sha256:e3ce8d66ac2121f8d476eb58f8bc50ab51336647615eb7cf514c21421cb818fd`	Os patches e as atualizações de segurança importantes.	23 de outubro de 2023	–

Versão do agente	Imagem de contêiner	Notas de release	Data de disponibilidade	Fim do suporte padrão [1]
v1.3.0	x86_64 (AMD64): `sha256:6dace2337dfbb7609811be89fb4b23ae0b865f1027ad78fbe69530bfbd46c694` Graviton (ARM64): `sha256:4928a7c6ef40e77c8ec95841323bb9a110db31f12c0ee7ab965e08b43efd01bb`	Compatível com a plataforma Ubuntu Compatível com o Kubernetes versão 1.28 Aprimoramentos gerais de performance e melhoria da estabilidade.	5 de outubro de 2023	–

Versão do agente	Imagem de contêiner	Notas de release	Data de disponibilidade	Fim do suporte padrão [1]
v1.2.0	x86_64 (AMD64): `sha256:d610413d662ec042057f05d6942496d7f2c08e9f5a077ea307ffdb5d3f11bcc3` Graviton (ARM64): `sha256:174d7ab28b2f95e5309da80d95b88ad26f602dfe72c2b351a0ef9297a1412bfa`	Além das instâncias baseadas em AMD64, a v1.2.0 agora também é compatível com instâncias baseadas em ARM64. Incluída e verificada a compatibilidade com o Bottlerocket Compatível com o Kubernetes versão 1.27 Aprimoramentos gerais de performance e melhorias de estabilidade.	16 de junho de 2023	–

Versão do agente	Imagem de contêiner	Notas de release	Data de disponibilidade	Fim do suporte padrão [1]
v1.1.0	`sha256:b19ba3a3c1a508d153263ae2fda891a7928b5ca9b3a5692db6c101829303281c`	Além do Versões do Kubernetes suportadas pelo agente de segurança GuardDuty , essa versão do agente também é compatível com a versão 1.26 do Kubernetes. Aprimoramentos gerais de performance e melhorias de estabilidade.	2 de maio de 2023	14 de maio de 2024
v1.0.0	`sha256:e38bdd2b1323e89113f1a31bd4bc8e5a8098525dd98e6981a28b9906b1e4411e`	Versão inicial do agente complementar do Amazon EKS.	30 de março de 2023	14 de maio de 2024

- [1] Para obter informações sobre a atualização da versão atual do agente que está chegando ao fim do suporte padrão, consulteAtualizando o agente de segurança manualmente.

Proteção do Amazon S3 na Amazon GuardDuty

O S3 Protection ajuda a Amazon a GuardDuty monitorar eventos de AWS CloudTrail dados do Amazon Simple Storage Service (Amazon S3) que incluem operações de API em nível de objeto para identificar possíveis riscos de segurança para dados em seus buckets do Amazon S3.

GuardDuty monitora eventos AWS CloudTrail de gerenciamento e eventos de dados do AWS CloudTrail S3 para identificar possíveis ameaças em seus recursos do Amazon S3. Essas fontes de dados monitoram diferentes tipos de atividade. Exemplos de eventos de CloudTrail gerenciamento para o S3 incluem operações que listam ou configuram buckets do Amazon S3, `ListBuckets` como`DeleteBuckets`, e. `PutBucketReplication` Exemplos de eventos de CloudTrail dados para o S3 incluem operações de API em nível de objeto, como`GetObject`,`ListObjects`, e. `DeleteObject` `PutObject`

Quando você habilita a Amazon GuardDuty para um Conta da AWS, GuardDuty começa a monitorar eventos CloudTrail de gerenciamento. Você não precisa ativar ou configurar manualmente o login de eventos de dados do S3. AWS CloudTrail Você pode ativar o recurso S3 Protection (que monitora eventos de CloudTrail dados para o S3) para qualquer conta em qualquer Região da AWS lugar em que esse recurso esteja disponível na Amazon GuardDuty, a qualquer momento. Um Conta da AWS que já tenha sido ativado GuardDuty, pode ativar o S3 Protection pela primeira vez com um período de teste gratuito de 30 dias. Para quem Conta da AWS é ativado pela primeira vez, o S3 Protection já está ativado e incluído neste teste gratuito de 30 dias. GuardDuty Para ter mais informações, consulte Estimando GuardDuty o custo.

Recomendamos que você ative a Proteção S3 no GuardDuty. Se esse recurso não estiver habilitado, não GuardDuty será possível monitorar totalmente seus buckets do Amazon S3 ou gerar descobertas de acesso suspeito aos dados armazenados em seus buckets do S3.

Como GuardDuty usa eventos de dados do S3

Quando você ativa os eventos de dados do S3 (Proteção do S3), GuardDuty começa a analisar os eventos de dados do S3 de todos os seus buckets do S3 e os monitora em busca de atividades maliciosas e suspeitas. Para ter mais informações, consulte AWS CloudTrail eventos de dados para S3.

Quando um usuário não autenticado acessa um objeto do S3, isso significa que o objeto do S3 está acessível ao público. Portanto, GuardDuty não processa essas solicitações. GuardDuty

processa as solicitações feitas aos objetos do S3 usando credenciais IAM (AWS Identity and Access Management) ou AWS STS (AWS Security Token Service) válidas.

Quando GuardDuty detecta uma ameaça potencial com base no monitoramento de eventos de dados do S3, ela gera uma descoberta de segurança. Para obter informações sobre os tipos de descobertas que GuardDuty podem ser geradas para os buckets do Amazon S3, consulte. GuardDuty Tipos de descoberta do S3

Se você desativar o S3 Protection, GuardDuty interromperá o monitoramento de eventos de dados do S3 dos dados armazenados em seus buckets do S3.

Como configurar a Proteção do S3 para uma conta independente

Para contas associadas por AWS Organizations, esse processo pode ser automatizado por meio das configurações do console. Para ter mais informações, consulte Como configurar a Proteção do S3 em ambientes de várias contas.

Para habilitar ou desabilitar a Proteção do S3

Selecione seu método de acesso preferido para configurar a Proteção do S3 para uma conta independente.

Console

1. Faça login no AWS Management Console e abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Proteção do S3.
3. A página Proteção do S3 fornece o status atual da Proteção do S3 para sua conta. É possível Habilitar ou Desabilitar a Proteção do S3 a qualquer momento.
4. Escolha Confirmar para confirmar sua seleção.

API/CLI

1. Execute updateDetector usando seu ID de detector válido para a região atual e passando o `name` do objeto `features` como `S3_DATA_EVENTS` definido para `ENABLED` ou `DISABLED` para habilitar ou desabilitar a Proteção do S3, respectivamente.

> **Note**
>
> Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

2. Como alternativa, você pode usar AWS Command Line Interface. Para habilitar a Proteção do S3, execute o comando a seguir e certifique-se de usar seu próprio ID de detector válido.

```
aws guardduty update-detector --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
features '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

Para desabilitar a Proteção do S3, substitua `ENABLED` por `DISABLED` no exemplo.

Como configurar a Proteção do S3 em ambientes de várias contas

Em um ambiente com várias contas, somente a conta do GuardDuty administrador delegado tem a opção de configurar (ativar ou desativar) a Proteção do S3 para as contas dos membros em sua organização. AWS As contas GuardDuty dos membros não podem modificar essa configuração em suas contas. A conta de GuardDuty administrador delegado gerencia suas contas de membros usando AWS Organizations. A conta de GuardDuty administrador delegado pode optar por ter o S3 Protection ativado automaticamente em todas as contas, somente em novas contas ou em nenhuma conta na organização. Para ter mais informações, consulte Gerenciando contas com o AWS Organizations.

Configurando o S3 Protection para uma conta de administrador delegado GuardDuty

Escolha seu método de acesso preferido para configurar o S3 Protection para a conta de GuardDuty administrador delegado.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de gerenciamento.
2. No painel de navegação, escolha Proteção do S3.
3. Na página Proteção do S3, escolha Editar.
4. Execute um destes procedimentos:

Como usar a opção Habilitar para todas as contas

- Escolha Habilitar para todas as contas. Isso habilitará o plano de proteção para todas as GuardDuty contas ativas em sua AWS organização, incluindo as novas contas que ingressam na organização.
- Escolha Salvar.

Como usar a opção Configurar contas manualmente

- Para habilitar o plano de proteção somente para a conta de GuardDuty administrador delegado, escolha Configurar contas manualmente.
- Escolha Habilitar na seção Conta de GuardDuty administrador delegado (esta conta).
- Selecione Salvar.

API/CLI

Execute updateDetectorusando o ID do detector da conta do GuardDuty administrador delegado da região atual e transmitindo o `features` objeto `name` como `S3_DATA_EVENTS` e `status` como `ENABLED` ou`DISABLED`.

Como alternativa, você pode configurar o S3 Protection usando o. AWS Command Line Interface*Execute o comando a seguir e certifique-se de substituir 12abc34d567e8fa901bc2d34e56789f0 pelo ID do detector da conta do administrador delegado da região atual e 5555555555 pelo ID da conta do administrador delegado. GuardDuty* Conta da AWS GuardDuty

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --account-ids 555555555555 --features '[{"Name": "RDS_LOGIN_EVENTS", "Status":
 "ENABLED"}]'
```

Habilite a Proteção do S3 para todas as contas-membro da organização

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Faça login usando sua conta de administrador.

2. Execute um destes procedimentos:

   Usando a página Proteção do S3

   1. No painel de navegação, escolha Proteção do S3.
   2. Escolha Habilitar para todas as contas. Essa ação habilita automaticamente a Proteção do S3 para contas novas e existentes na organização.
   3. Escolha Salvar.

   > **Note**
   >
   > Pode levar até 24 horas para atualizar a configuração das contas-membro.

   Como usar a página Contas

   1. No painel de navegação, escolha Accounts (Contas).
   2. Na página Contas, escolha Habilitar automaticamente as preferências antes de Adicionar contas por convite.
   3. Na janela Gerenciar preferências de habilitação automática, escolha Habilitar para todas as contas em Proteção do S3.
   4. Escolha Salvar.

   Se você não conseguir usar a opção Habilitar para todas as contas, consulte Habilite ou desabilite seletivamente a Proteção do S3 nas contas-membro.

API/CLI

- *Para habilitar ou desabilitar seletivamente a Proteção do S3 para suas contas-membro, invoque a operação da API updateMemberDetectors usando seu próprio ID de detector.*
- O exemplo a seguir mostra como você pode habilitar a Proteção do S3 para uma conta de membro único. *Certifique-se de substituir 12abc34d567e8fa901bc2d34e56789f0 pela conta do administrador delegado e 111122223333. detector-id GuardDuty* Para desabilitar a Proteção S3, substitua `ENABLED` por `DISABLED`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
 '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
```

  > **Note**
  >
  > Você também pode passar uma lista de IDs de contas separadas por um espaço.

- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Habilite a Proteção S3 para todas as contas-membro ativas existentes

Escolha seu método de acesso preferido para habilitar a Proteção do S3 para todas as contas-membro ativas existentes em sua organização.

Console

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

   Faça login usando as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, escolha Proteção do S3.

3. Na página Proteção do S3, é possível exibir o status atual da configuração. Na seção Contas-membro ativas, escolha Ações.
4. No menu suspenso Ações, escolha Habilitar para todas as contas-membro ativas existentes.
5. Selecione a opção Confirmar.

API/CLI

- *Para habilitar ou desabilitar seletivamente a Proteção do S3 para suas contas-membro, invoque a operação da API updateMemberDetectors usando seu próprio ID de detector.*
- O exemplo a seguir mostra como você pode habilitar a Proteção do S3 para uma conta de membro único. *Certifique-se de substituir 12abc34d567e8fa901bc2d34e56789f0 pela conta do administrador delegado e 111122223333. detector-id GuardDuty* Para desabilitar a Proteção S3, substitua `ENABLED` por `DISABLED`.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-member-detectors --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 111122223333 --features
   '[{"name": "S3_DATA_EVENTS", "status": "ENABLED"}]'
  ```

  > **Note**
  >
  > Você também pode passar uma lista de IDs de contas separadas por um espaço.

- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Habilite automaticamente a proteção S3 para contas de novos membros

Selecione seu método de acesso preferido para habilitar a Proteção do S3 para novas contas que ingressam na sua organização.

Console

A conta de GuardDuty administrador delegado pode habilitar novas contas de membros em uma organização por meio do console, usando a página Proteção do S3 ou Contas.

Para habilitar automaticamente a Proteção do S3 para novas contas-membro

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.

2. Execute um destes procedimentos:

   - Usando a página Proteção do S3:

     1. No painel de navegação, escolha Proteção do S3.
     2. Na página Proteção do S3, escolha Editar.
     3. Escolha Configurar contas manualmente.
     4. Selecione Habilitar automaticamente para novas contas-membro. Essa etapa garante que sempre que uma nova conta ingressar na sua organização, a Proteção do S3 seja habilitada automaticamente para a conta dessa pessoa. Somente a conta do GuardDuty administrador delegado da organização pode modificar essa configuração.
     5. Selecione Salvar.

   - Como usar a página Contas:

     1. No painel de navegação, escolha Accounts (Contas).
     2. Na página Contas, escolha Habilitar automaticamente as preferências.
     3. Na janela Gerenciar preferências de habilitação automática, selecione Habilitar para novas contas em Proteção do S3.
     4. Escolha Salvar.

API/CLI

- Para habilitar ou desabilitar seletivamente a Proteção do S3 para suas contas-membro, invoque a operação da API UpdateOrganizationConfiguration usando seu próprio *`ID de detector`*.
- O exemplo a seguir mostra como você pode habilitar a Proteção do S3 para uma conta de membro único. Para desabilitá-lo, consulte Habilitar ou desabilitar seletivamente a Proteção do RDS para contas-membro. Defina as preferências para habilitar ou desabilitar automaticamente

o plano de proteção nessa região para novas contas (`NEW`) que ingressam na organização, todas as contas (`ALL`) ou nenhuma das contas (`NONE`) na organização. Para obter mais informações, consulte autoEnableOrganizationMembros. Com base na sua preferência, talvez seja necessário substituir `NEW` por `ALL` ou `NONE`.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty update-organization-configuration --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable --features '[{"Name":
 "S3_DATA_EVENTS", "autoEnable": "NEW"}]'
```

> **Note**
>
> Você também pode passar uma lista de IDs de contas separadas por um espaço.

- Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

Habilite ou desabilite seletivamente a Proteção do S3 nas contas-membro

Escolha seu método de acesso preferido para habilitar ou desabilitar seletivamente a Proteção do S3 para contas-membro.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar as credenciais da conta de GuardDuty administrador delegado.

2. No painel de navegação, escolha Accounts (Contas).

   Na página Contas, analise a coluna Proteção do S3 para ver o status da sua conta-membro.

3. Para habilitar ou desabilitar seletivamente a Proteção do S3

   Selecione a conta para a qual deseja configurar a Proteção do S3. Você pode selecionar várias contas ao mesmo tempo. No menu suspenso Editar planos de proteção, selecione S3Pro e escolha a opção apropriada.

API/CLI

Para habilitar ou desabilitar seletivamente a Proteção do S3 para suas contas-membro, execute a operação da API updateMemberDetectors usando seu próprio ID de detector. O exemplo a seguir mostra como você pode habilitar a Proteção do S3 para uma conta de membro único. Para desabilitá-la, substitua `true` por `false`.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
 aws guardduty update-member-detectors --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --account-ids 123456789012 --features
 '[{"Name" : "S3_DATA_EVENTS", "Status" : "ENABLED"}]'
```

> **Note**
>
> Você também pode passar uma lista de IDs de contas separadas por um espaço.

Quando o código é executado com êxito, ele retorna uma lista vazia de `UnprocessedAccounts`. Se houver algum problema na alteração das configurações do detector de uma conta, esse ID de conta será listado junto com um resumo do problema.

> **Note**
>
> Se você usa scripts para integrar novas contas e deseja desabilitar a Proteção do S3 em suas novas contas, você pode modificar a operação da API createDetector com o objeto `dataSources` opcional, conforme descrito neste tópico.

Desativando automaticamente o S3 Protection para novas contas GuardDuty

> **Important**
>
> Por padrão, o S3 Protection é ativado automaticamente para Contas da AWS essa união GuardDuty pela primeira vez.

Se você tiver uma conta de GuardDuty administrador ativada GuardDuty pela primeira vez em uma nova conta e não quiser que o S3 Protection seja ativado por padrão, você pode desativá-lo modificando a operação da createDetectorAPI com o objeto opcional`features`. O exemplo a seguir usa o AWS CLI para ativar um novo GuardDuty detector com a Proteção S3 desativada.

```
aws guardduty create-detector --enable --features '[{"Name" : "S3_DATA_EVENTS",
"Status" : "DISABLED"}]'
```

Atributo na Proteção do S3

AWS CloudTrail eventos de dados para S3

Eventos de dados, também conhecidos como operações do plano de dados, fornecem insights sobre as operações de recurso executadas no recurso ou dentro de um recurso. Muitas vezes, são atividades de grande volume.

Veja a seguir exemplos de eventos de CloudTrail dados para o S3 que GuardDuty podem ser monitorados:

- Operações da API `GetObject`
- Operações da API `PutObject`
- Operações da API `ListObjects`
- Operações da API `DeleteObject`

Quando você ativa GuardDuty pela primeira vez, o S3 Protection é ativado por padrão e também está incluído no período de teste gratuito de 30 dias. No entanto, esse recurso é opcional e você pode optar por habilitá-lo ou desabilitá-lo para qualquer conta ou região a qualquer momento. Para obter mais informações sobre a configuração do Amazon S3 como um atributo, consulte GuardDuty Proteção S3.

Entendendo as GuardDuty descobertas da Amazon

Uma GuardDuty descoberta representa um possível problema de segurança detectado em sua rede. GuardDutygera uma descoberta sempre que detecta atividades inesperadas e potencialmente maliciosas em seu AWS ambiente.

Você pode visualizar e gerenciar suas GuardDuty descobertas na página Descobertas no GuardDuty console ou usando as AWS CLI operações da API. Para uma visão geral das formas de gerenciar descobertas, consulte Gerenciando as GuardDuty descobertas da Amazon.

Tópicos

Detalhes da descoberta

No GuardDuty console da Amazon, você pode ver os detalhes da descoberta na seção de resumo da descoberta. Os detalhes da descoberta variam de acordo com o tipo de descoberta.

Há dois detalhes principais que determinarão quais tipos de informações serão disponibilizadas para qualquer descoberta. O primeiro é o tipo de recurso, que pode ser `Instance`, `AccessKey`, `S3Bucket`, `Kubernetes cluster`, `ECS cluster`, `Container`, `RDSDBInstance` ou `Lambda`. O segundo detalhe que determina as informações da descoberta é a Função do recurso. A função do recurso pode ser `Target` para chaves de acesso, o que significa que o recurso foi alvo de atividades

suspeitas. Por exemplo, tipo de descoberta, a função do recurso também pode ser `Actor`, o que significa que seu recurso foi o agente que realizou atividades suspeitas. Este tópico descreve alguns dos detalhes geralmente disponíveis sobre descobertas.

Visão geral da descoberta

A seção Visão geral de uma descoberta contém os atributos de identificação mais básicos da descoberta, incluindo as seguintes informações:

- ID da conta — A ID da AWS conta na qual a atividade ocorreu que solicitou GuardDuty a geração dessa descoberta.
- Contagem — O número de vezes GuardDuty que agregou uma atividade que corresponde a esse padrão a essa ID de descoberta.
- Criada em: a data e hora em que esta descoberta foi criada pela primeira vez. Se esse valor for diferente de Atualizado em indica que a atividade ocorreu várias vezes e é um problema contínuo.

> **Note**
>
> Os carimbos de data e hora das descobertas no GuardDuty console aparecem em seu fuso horário local, enquanto as exportações JSON e as saídas de CLI exibem carimbos de data e hora em UTC.

- ID da descoberta: um ID exclusivo para este tipo de descoberta e conjunto de parâmetros. Novas ocorrências de atividades que correspondem a esse padrão serão agregadas ao mesmo ID.
- Tipo de descoberta: uma string formatada representando o tipo de atividade que acionou a descoberta. Para ter mais informações, consulte Formato de busca do GuardDuty.
- Região — A AWS região na qual a descoberta foi gerada. Para obter mais informações sobre as regiões compatíveis, consulte Regiões e endpoints
- ID do recurso — O ID do AWS recurso contra o qual a atividade ocorreu e que solicitou GuardDuty a geração dessa descoberta.
- ID do escaneamento — Aplicável às descobertas quando a Proteção contra GuardDuty Malware está ativada, esse é um identificador do escaneamento de malware executado nos volumes do EBS conectados à instância EC2 ou carga de trabalho do contêiner potencialmente comprometida. Para ter mais informações, consulte Detalhes de descobertas sobre a Proteção contra malware.
- Gravidade: o nível de gravidade atribuído à descoberta, que pode ser Alta, Média ou Baixa. Para ter mais informações, consulte Níveis de severidade GuardDuty das descobertas.

- Atualizado em — A última vez que essa descoberta foi atualizada com uma nova atividade correspondente ao padrão que levou GuardDuty à geração dessa descoberta.

Recurso

O recurso afetado fornece detalhes sobre o AWS recurso que foi alvo da atividade inicial. As informações disponíveis variam de acordo com o tipo de recurso e o tipo de ação.

Função do recurso — A função do AWS recurso que iniciou a descoberta. Esse valor pode ser TARGET ou ACTOR, e representa se seu recurso foi o alvo da atividade suspeita ou o ator que realizou a atividade suspeita, respectivamente.

Tipo de recurso: o tipo de recurso afetado. Se houver vários recursos envolvidos, uma descoberta poderá incluir vários tipos de recursos. Os tipos de recursos são Instance, S3Bucket AccessKey, ECSCluster, Container KubernetesCluster, RDSDBInstance e Lambda. Dependendo do tipo de recurso, diferentes detalhes da descoberta estarão disponíveis. Selecione uma guia de opções do recurso para saber mais sobre os detalhes disponíveis para ele.

Instance

Detalhes da instância:

> **Note**
>
> Alguns detalhes da instância podem estar ausentes se a instância já tiver sido interrompida ou se a invocação da API subjacente tiver se originado de uma instância do EC2 em uma região diferente ao fazer uma chamada de API entre regiões.

- ID da instância — A ID da instância do EC2 envolvida na atividade que solicitou GuardDuty a geração da descoberta.
- Tipo de instância: o tipo de instância do EC2 envolvida na descoberta.
- Hora de execução: a data e a hora em que a instância foi executada.
- Outpost ARN — O nome de recurso da Amazon (ARN) de. AWS Outposts Aplicável somente às AWS Outposts instâncias. Para ter mais informações, consulte O que é o AWS Outposts?
- Nome do grupo de segurança: o nome do grupo de segurança anexado à instância envolvida.
- ID do grupo de segurança: o ID do grupo de segurança anexado à instância envolvida.

- Estado da instância: o estado atual da instância de destino.
- Zona de disponibilidade: a zona de disponibilidade da região da AWS em que a instância envolvida está localizada.
- ID da imagem: o ID da imagem de máquina da Amazon usada para criar a instância envolvida na atividade.
- Descrição da imagem: uma descrição do ID da imagem de máquina da Amazon usada para criar a instância envolvida na atividade.
- Tags: uma lista de tags anexadas a este recurso, listadas no formato de `key:value`.

AccessKey

Detalhes da chave de acesso:

- ID da chave de acesso — A ID da chave de acesso do usuário envolvido na atividade que solicitou GuardDuty a geração da descoberta.
- ID principal — A ID principal do usuário envolvido na atividade que levou GuardDuty à geração da descoberta.
- Tipo de usuário — O tipo de usuário envolvido na atividade que levou GuardDuty à geração da descoberta. Para obter mais informações, consulte Elemento userIdentity do CloudTrail .
- Nome de usuário — O nome do usuário envolvido na atividade que levou GuardDuty à geração da descoberta.

S3Bucket

Detalhes do bucket Amazon S3:

- Nome: o nome do bucket envolvido na descoberta.
- ARN: o ARN do bucket envolvido na descoberta.
- Proprietário: o ID de usuário canônico do usuário que possui o bucket envolvido na descoberta. Para obter mais informações sobre IDs de usuário canônicos, consulte Identificadores de conta da AWS.
- Tipo: o tipo de descoberta do bucket, pode ser Destino ou Origem.
- Criptografia padrão do lado do servidor: os detalhes de criptografia para o bucket.
- Tags de bucket: uma lista de tags anexadas a esse recurso, listadas no formato de `key:value`.

- Permissões efetivas: uma avaliação de todas as permissões e políticas efetivas no bucket que indica se o bucket envolvido está exposto publicamente. Os valores podem ser públicos ou não públicos.

EKSCluster

Detalhes do cluster do Kubernetes:

- Nome: o nome do cluster do Kubernetes.
- ARN: o ARN que identifica o cluster.
- Criado em: a data e a hora em que o cluster foi criado.

> **Note**
>
> Os carimbos de data e hora das descobertas no GuardDuty console aparecem em seu fuso horário local, enquanto as exportações JSON e as saídas de CLI exibem carimbos de data e hora em UTC.

- VPC ID: o ID da VPC associada ao cluster.
- Status: o status atual do cluster.
- Tags: os metadados que você aplica ao cluster para ajudar na categorização e organização. Cada tag consiste em uma chave e um valor opcional, listados no formato `key:value`. Você pode definir a chave e o valor.

  As tags de cluster não são propagadas para nenhum outro recurso associado ao cluster.

Detalhes da workload do Kubernetes:

- Tipo: o tipo de workload do Kubernetes, como pod, implantação e trabalho.
- Nome: o nome da workload do Kubernetes.
- Uid: o ID exclusivo da workload do Kubernetes.
- Criada em: a data e a hora em que essa workload foi criada.
- Rótulos: os pares de chave-valor anexados à workload do Kubernetes.
- Contêineres: os detalhes do contêiner em execução como parte da workload do Kubernetes.
- Namespace: a workload pertence a esse namespace do Kubernetes.
- Volumes: os volumes usados pela workload do Kubernetes.

    - Caminho do host: representa um arquivo ou diretório preexistente na máquina host para a qual o volume é mapeado.
    - Nome: o nome do volume.
- contexto de segurança do pod: define as configurações de privilégio e controle de acesso para todos os contêineres em um pod.
- Rede de host: defina como `true` se os pods estão incluídos na workload do Kubernetes.

Detalhes do usuário do Kubernetes:

- Grupos: grupos com RBAC (controle baseado em acesso por função) do Kubernetes do usuário envolvido na atividade que gerou a descoberta.
- ID: ID exclusiva do usuário do Kubernetes.
- Nome de usuário: nome do usuário do Kubernetes envolvido na atividade que gerou a descoberta.
- Nome da sessão: entidade que assumiu o perfil do IAM com permissões RBAC do Kubernetes.

ECSCluster

Detalhes do cluster do ECS:

- ARN: o ARN que identifica o cluster.
- Nome: o nome do cluster.
- Status: o status atual do cluster.
- Contagem de serviços ativas: o número de serviços que estão sendo executados no cluster em um estado `ACTIVE`. Você pode ver esses serviços com ListServices
- Contagem de instâncias de contêiner registradas: o número de instâncias de contêiner registradas no cluster. Isso inclui instâncias de contêiner nos status `ACTIVE` e `DRAINING`.
- Contagem de tarefas em execução: o número de tarefas no cluster que estão no estado `RUNNING`.
- Tags: os metadados que você aplica ao cluster para ajudar na categorização e organização. Cada tag consiste em uma chave e um valor opcional, listados no formato `key:value`. Você pode definir a chave e o valor.
- Contêineres: os detalhes sobre o contêiner associado à tarefa:
    - Nome do contêiner: o nome do contêiner.

    - Imagem do contêiner: a imagem do contêiner.
- Detalhes da tarefa: os detalhes de uma tarefa em um cluster.
    - ARN: o nome do recurso da Amazon (ARN) da tarefa.
    - ARN da definição: o nome do recurso da Amazon (ARN) da definição de tarefa que cria a tarefa.
    - Versão: o contador de versões da tarefa.
    - Tarefa criada em: a data e hora do Unix quando a tarefa foi criada.
    - Tarefa iniciada em: a data e hora do Unix quando a tarefa foi iniciada.
    - Tarefa iniciada por: a tag especificada quando uma tarefa é iniciada.

Container

Detalhes do contêiner:

- Runtime do contêiner: o runtime do contêiner (como `docker` ou `containerd`) usado para executar o contêiner.
- ID: o ID da instância de contêiner ou as entradas completas do ARN para a instância de contêiner.
- Nome: o nome do contêiner.

  Quando disponível, esse campo exibe o valor do rótulo `io.kubenetes.container.name`.
- Imagem: a imagem da instância de contêiner.
- Montagens de volume: lista de montagens de volume de contêineres. Um contêiner pode montar um volume em seu sistema de arquivos.
- Contexto de segurança: o contexto de segurança do contêiner define as configurações de privilégio e controle de acesso para um contêiner.
- Detalhes do processo: descreve os detalhes do processo associado à descoberta.

RDSDBInstance

Detalhes da instância do RDSDB:

> **Note**
>
> Esse recurso está disponível nas descobertas da Proteção do RDS relacionadas à instância do banco de dados.

- ID da instância do banco de dados — O identificador associado à instância do banco de dados envolvida na GuardDuty descoberta.
- Mecanismo: o nome do mecanismo de banco de dados da instância do banco de dados envolvida na descoberta. Os valores permitidos são Aurora compatível com MySQL ou Aurora PostgreSQL.
- Versão do mecanismo — A versão do mecanismo de banco de dados envolvida na GuardDuty descoberta.
- ID do cluster do banco de dados — O identificador do cluster do banco de dados que contém o ID da instância do banco de dados envolvido na GuardDuty descoberta.
- ARN da instância do banco de dados — O ARN que identifica a instância do banco de dados envolvida na descoberta. GuardDuty

Lambda

Detalhes da função do Lambda

- Nome da função: o nome da função do Lambda que está envolvida na descoberta.
- Versão da função: a versão da função do Lambda envolvida na descoberta.
- Descrição da função: uma descrição da função do Lambda envolvida na descoberta.
- ARN da função: o nome do recurso da Amazon (ARN) da função do Lambda envolvida na descoberta.
- ID da revisão: o ID da revisão da versão da função do Lambda.
- Perfil: o perfil de execução da função do Lambda envolvida na descoberta.
- Configuração da VPC: a configuração da Amazon VPC, incluindo o ID da VPC, o grupo de segurança e as IDs de sub-rede associadas à sua função do Lambda.
- ID da VPC: o ID da Amazon VPC associado à função do Lambda envolvida na descoberta.
- IDs de sub-rede: o ID das sub-redes associadas à sua função do Lambda.

- Grupo de segurança: o grupo de segurança vinculado à função do Lambda envolvida. Inclui o nome do grupo de segurança e o ID do grupo.
- Tags: uma lista de tags anexadas a este recurso, listadas no formato de par de `key:value`.

Detalhes do usuário do banco de dados (DB) do RDS

> **Note**
>
> Esta seção é aplicável às descobertas quando você ativa o recurso de Proteção do RDS no GuardDuty. Para ter mais informações, consulte GuardDuty Proteção RDS.

A GuardDuty descoberta fornece os seguintes detalhes de usuário e autenticação do banco de dados potencialmente comprometido.

- Usuário: o nome de usuário usado para fazer a tentativa anômala de login.
- Aplicação: o nome da aplicação usada para fazer a tentativa anômala de login.
- Banco de dados: o nome da instância do banco de dados envolvida na tentativa anômala de login.
- SSL: a versão do Secure Socket Layer (SSL) usada para a rede.
- Método de autenticação: o método de autenticação usado pelo usuário envolvido na descoberta.

Detalhes da descoberta do Runtime Monitor

> **Note**
>
> Esses detalhes podem estar disponíveis somente se GuardDuty gerar um dosTipos de descoberta de monitoramento de tempo de execução.

Esta seção contém os detalhes do runtime, como detalhes do processo e qualquer contexto necessário. Os detalhes do processo descrevem as informações sobre o processo observado e o contexto do runtime descreve qualquer informação adicional sobre a atividade potencialmente suspeita.

Detalhes do processo

- Nome: o nome do processo.
- Caminho do executável: o caminho absoluto do arquivo executável do processo.
- SHA-256 do executável: o hash `SHA256` do executável do processo.
- PID do Namespace: o ID do processo em um namespace PID secundário diferente do namespace PID no nível do host. Para processos em um contêiner, é o ID do processo observado dentro do contêiner.
- Diretório de trabalho atual: o diretório de trabalho atual do processo.
- ID do processo: o ID atribuído ao processo pelo sistema operacional.
- startTime: a hora em que o processo foi iniciado. Está no formato de string de data UTC (`2023-03-22T19:37:20.168Z`).
- UUID — O ID exclusivo atribuído ao processo por. GuardDuty
- UUID principal: o ID exclusivo do processo principal. Essa ID é atribuída ao processo principal por GuardDuty.
- Usuário: o usuário que executou o processo.
- ID do usuário: o ID do usuário que executou o processo.
- ID de usuário efetivo: o ID de usuário efetivo do processo no momento do evento.
- Linhagem: informações sobre os ancestrais do processo.
  - ID do processo: o ID atribuído ao processo pelo sistema operacional.
  - UUID — O ID exclusivo atribuído ao processo por. GuardDuty
  - Caminho do executável: o caminho absoluto do arquivo executável do processo.
  - ID de usuário efetivo: o ID de usuário efetivo do processo no momento do evento.
  - UUID principal: o ID exclusivo do processo principal. Essa ID é atribuída ao processo principal por GuardDuty.
  - Hora de início: o hora em que o processo foi iniciado.
  - PID do Namespace: o ID do processo em um namespace PID secundário diferente do namespace PID no nível do host. Para processos em um contêiner, é o ID do processo observado dentro do contêiner.
  - ID do usuário: o ID do usuário que executou o processo.
  - Nome: o nome do processo.

Contexto de runtime

Com os campos a seguir, uma descoberta gerada pode incluir somente os campos relevantes para o tipo de descoberta.

- Origem de montagem: o caminho no host que é montado pelo contêiner.
- Destino de montagem: o caminho no contêiner que é mapeado para o diretório do host.
- Tipo de sistema de arquivos: representa o tipo do sistema de arquivos montado.
- Sinalizadores: representam opções que controlam o comportamento do evento envolvido nessa descoberta.
- Processo de modificação: informações sobre o processo que criou ou modificou um binário, script ou biblioteca dentro de um contêiner no runtime.
- Modificado em: o carimbo de data/hora em que o processo criou ou modificou um binário, script ou biblioteca dentro de um contêiner no runtime. Esse campo está no formato de string de data UTC (`2023-03-22T19:37:20.168Z`).
- Caminho da biblioteca: o caminho para a nova biblioteca que foi carregada.
- Valor de LD Preload: o valor da variável de ambiente `LD_PRELOAD`.
- Caminho do soquete: o caminho para o soquete do Docker que foi acessado.
- Caminho do binário Runc: o caminho para o binário `runc`.
- Caminho do agente de liberação: o caminho para o arquivo do agente de liberação `cgroup`.
- Exemplo de linha de comando — O exemplo da linha de comando envolvida na atividade potencialmente suspeita.
- Categoria da ferramenta — Categoria à qual a ferramenta pertence. Alguns dos exemplos são Backdoor Tool, Pentest Tool, Network Scanner e Network Sniffer.
- Nome da ferramenta — O nome da ferramenta potencialmente suspeita.
- Caminho do script — O caminho para o script executado que gerou a descoberta.
- Caminho do arquivo da ameaça — O caminho suspeito para o qual os detalhes da inteligência da ameaça foram encontrados.
- Nome do serviço — O nome do serviço de segurança que foi desativado.

Detalhes de verificação de volumes do EBS

> **Note**
>
> Esta seção é aplicável às descobertas quando você ativa a verificação de GuardDuty malware iniciada emGuardDuty Proteção contra malware.

A análise de volumes do EBS fornece detalhes sobre o volume do EBS anexado à instância EC2 ou à workload do contêiner potencialmente comprometida.

- ID da verificação: o identificador da verificação de malware.
- Verificação começou em: a data e a hora em que a verificação de malware foi iniciado.
- Verificação concluída em: a data e hora em que foi concluída a verificação de malware.
- Trigger Finding ID — O ID de GuardDuty descoberta da descoberta que iniciou essa verificação de malware.
- Fontes:: os valores possíveis são `Bitdefender` e `AWS`.
- Detecções de verificações: a visão completa dos detalhes e resultados de cada verificação de malware.
  - Contagem de itens verificados: o número total de arquivos verificados. Fornece detalhes como `totalGb`, `files` e `volumes`.
  - Contagem de itens detectados por ameaças: o número total de `files` mal-intencionados detectados durante a verificação.
  - Detalhes da ameaça de maior gravidade: os detalhes da ameaça de maior gravidade detectada durante a verificação e o número de arquivos mal-intencionados. Fornece detalhes como `severity`, `threatName` e `count`.
  - Ameaças detectadas por nome: o elemento de contêiner que agrupa ameaças de todos os níveis de gravidade. Fornece detalhes como `itemCount`, `uniqueThreatNameCount`,`shortened` e `threatNames`.

Detalhes de descobertas sobre a Proteção contra malware

> **Note**
>
> Esta seção é aplicável às descobertas quando você ativa a verificação de GuardDuty malware iniciada emGuardDuty Proteção contra malware.

Quando o verificação da Proteção contra malware detecta malware, você pode ver os detalhes do verificação selecionando a descoberta correspondente na página Descobertas no console https://console.aws.amazon.com/guardduty/. A gravidade da descoberta sobre a Proteção contra Malware depende da gravidade da GuardDuty descoberta.

> **Note**
>
> A tag `GuardDutyFindingDetected` especifica que os snapshots contêm malware.

As informações exibidas a seguir estão disponíveis na seção Ameaças detectadas no painel de detalhes.

- Nome: o nome da ameaça, obtido ao agrupar os arquivos por detecção.
- Gravidade: a gravidade da ameaça detectada.
- Hash: o hash SHA-256 do arquivo.
- Caminho do arquivo: a localização do arquivo mal-intencionado no volume do EBS.
- Nome do arquivo: o nome do arquivo em que a ameaça foi detectada.
- ARN do volume: o ARN dos volumes do EBS verificados.

As informações a seguir estão disponíveis na seção Detalhes do verificação de malware no painel de detalhes.

- ID de verificação: o ID de verificação da verificação de malware.
- Verificação começou em: a data e a hora em que a verificação foi iniciada.
- Verificação concluída em: a data e a hora em que a verificação foi concluída.
- Arquivos verificados: o número total de arquivos e diretórios verificados.

- Total de GB verificados: a quantidade de armazenamento verificada durante o processo.
- ID de descoberta do gatilho — O ID de GuardDuty descoberta da descoberta que iniciou essa verificação de malware.
- As informações exibidas a seguir estão disponíveis na seção Detalhes do volume no painel de detalhes.
  - ARN do volume: o nome do recurso da Amazon (ARN) do volume.
  - SnapshotARN: o ARN do snapshot do volume do EBS.
  - Status: o status de verificação do volume, como`Running`, `Skipped` e `Completed`.
  - Tipo de criptografia: o tipo de criptografia usado para criptografar o volume. Por exemplo, `CMCMK`.
  - Nome do dispositivo: o nome do dispositivo. Por exemplo, `/dev/xvda`.

Ação

A Ação de uma descoberta fornece detalhes sobre o tipo de atividade que acionou a descoberta. As informações disponíveis variam com base no tipo de ação.

Tipo de ação: o tipo de atividade de descoberta. Esse valor pode ser NETWORK_CONNECTION, PORT_PROBE, DNS_REQUEST, AWS_API_CALL ou RDS_LOGIN_ATTEMPT. As informações disponíveis variam com base no tipo de ação:

- NETWORK_CONNECTION: indica que o tráfego de rede foi trocado entre a instância do EC2 identificada e o host remoto. Esse tipo de ação tem as seguintes informações adicionais:
  - Direção da conexão — A direção da conexão de rede observada na atividade que levou GuardDuty à geração da descoberta. Os valores podem ser:
    - INBOUND: indica que um host remoto iniciou uma conexão a uma porta local na instância do EC2 identificada na conta.
    - OUTBOUND: indica que a instância do EC2 identificada iniciou uma conexão a um host remoto.
    - DESCONHECIDO — Indica que não GuardDuty foi possível determinar a direção da conexão.
  - Protocolo — O protocolo de conexão de rede observado na atividade que levou GuardDuty à geração da descoberta.
  - IP local: o endereço IP de origem original do tráfego que acionou a descoberta. Essas informações podem ser usadas para fazer a distinção entre o endereço IP de uma camada

intermediária pela qual o tráfego flui e o endereço IP de origem original do tráfego que acionou a descoberta. Por exemplo, o endereço IP de um pod do EKS em oposição ao endereço IP da instância em que o pod do EKS está sendo executado.

- Bloqueado: indica se a porta de destino está bloqueada.

- PORT_PROBE: indica que um host remoto consultou a instância do EC2 identificada em várias portas abertas. Esse tipo de ação tem as seguintes informações adicionais:
  - IP local: o endereço IP de origem original do tráfego que acionou a descoberta. Essas informações podem ser usadas para fazer a distinção entre o endereço IP de uma camada intermediária pela qual o tráfego flui e o endereço IP de origem original do tráfego que acionou a descoberta. Por exemplo, o endereço IP de um pod do EKS em oposição ao endereço IP da instância em que o pod do EKS está sendo executado.
  - Bloqueado: indica se a porta de destino está bloqueada.
- DNS_REQUEST: indica que a instância do EC2 identificada consultou um nome de domínio. Esse tipo de ação tem as seguintes informações adicionais:
  - Protocolo — O protocolo de conexão de rede observado na atividade que levou GuardDuty à geração da descoberta.
  - Bloqueado: indica se a porta de destino está bloqueada.
- AWS_API_CALL: indica que uma API da AWS foi invocada. Esse tipo de ação tem as seguintes informações adicionais:
  - API — O nome da operação de API que foi invocada e, portanto, solicitada GuardDuty para gerar essa descoberta.

    > **Note**
    >
    > Essas operações também podem incluir eventos que não são de API capturados pelo AWS CloudTrail. Para obter mais informações, consulte Eventos não relacionados à API capturados por CloudTrail.

  - Agente do usuário: o agente do usuário que fez a solicitação da API. Esse valor informa se a chamada foi feita a partir do AWS Management Console, de um AWS serviço, dos AWS SDKs ou do AWS CLI.
  - CÓDIGO DE ERRO: se a descoberta foi acionada por uma falha na chamada de API, o código de erro dessa chamada será exibido.
  - Nome do serviço: o nome DNS do serviço que tentou fazer a chamada de API que acionou a descoberta.

- RDS_LOGIN_ATTEMPT: indica que foi feita uma tentativa de login no banco de dados potencialmente comprometido de um endereço IP remoto.
  - Endereço IP: o endereço IP remoto usado para fazer a tentativa de login potencialmente suspeita.

Agente ou destino

Uma descoberta terá uma seção Agente se a Função do recurso for `TARGET`. Isso indicará que o recurso foi alvo de atividades suspeitas, e a seção Agente apresentará detalhes sobre a entidade que apontou para o recurso.

Uma descoberta terá uma seção Destino se a Função do recurso for `ACTOR`. Isso indica que o recurso estava envolvido em atividades suspeitas em um host remoto, e essa seção contém informações sobre o IP e/ou domínio para o qual o recurso apontou.

As informações disponíveis em uma seção Agente ou Destino podem incluir:

- Afiliado — Detalhes sobre se a AWS conta do chamador remoto da API está relacionada ao seu GuardDuty ambiente. Se esse valor for `true`, o chamador da API está afiliado à sua conta de alguma forma. Se for `false`, o chamador da API é de fora do seu ambiente.
- ID da conta remota — A ID da conta que possui o endereço IP de saída usado para acessar o recurso na rede final.
- Endereço IP — O endereço IP envolvido na atividade que levou GuardDuty à geração da descoberta.
- Localização — Informações de localização do endereço IP envolvido na atividade que levou GuardDuty à geração da descoberta.
- Organização — informações da organização do ISP sobre o endereço IP envolvido na atividade que levou GuardDuty à geração da descoberta.
- Porta — O número da porta envolvida na atividade que levou GuardDuty à geração da descoberta.
- Domínio — O domínio envolvido na atividade que levou GuardDuty à geração da descoberta.
- Domínio com sufixo — O domínio de segundo e primeiro nível envolvido em uma atividade que potencialmente levou GuardDuty à geração da descoberta. Para obter uma lista de domínios de primeiro e segundo nível, consulte a lista pública de sufixos.

Mais informações

Todas as descobertas têm uma seção Informações adicionais que pode incluir as seguintes informações:

- Nome da lista de ameaças — O nome da lista de ameaças que inclui o endereço IP ou o nome de domínio envolvido na atividade que levou GuardDuty à geração da descoberta.
- Amostra: um valor verdadeiro ou falso que indica se é uma descoberta de amostra.
- Arquivada: um valor verdadeiro ou falso que indica se essa descoberta foi arquivada.
- Incomum: detalhes da atividade que não foram observados historicamente. Eles podem incluir um usuário, local, hora, bucket, comportamento de login ou ASN Org incomum (não observado anteriormente).
- Protocolo incomum — O protocolo de conexão de rede envolvido na atividade que levou GuardDuty à geração da descoberta.
- Detalhes do agente: detalhes sobre o agente de segurança que está atualmente implantado no cluster do EKS em sua Conta da AWS. Isso só se aplica aos tipos de descoberta do Monitoramento de runtime do EKS.
  - Versão do agente — A versão do agente GuardDuty de segurança.
  - ID do agente — O identificador exclusivo do agente GuardDuty de segurança.

Evidência

As descobertas baseadas na inteligência de ameaças têm uma seção Evidência que inclui as seguintes informações:

- Detalhes da inteligência de ameaças — O nome da lista de ameaças na qual as ameaças reconhecidas `Threat name` aparecem.
- Nome da ameaça — O nome da família de malware ou outro identificador associado à ameaça.
- Arquivo de ameaça SHA256 — SHA256 do arquivo que gerou a descoberta.

Comportamento anômalo

Os tipos de descobertas que terminam em AnomalousBehaviorindicam que a descoberta foi gerada pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de machine learning avalia todas as solicitações de API para sua conta e identifica eventos anômalos

associados às táticas usadas pelos adversários. O modelo de machine learning rastreia vários fatores da solicitação de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e a API específica que foi solicitada.

Detalhes sobre quais fatores da solicitação de API são incomuns para a identidade CloudTrail do usuário que invocou a solicitação podem ser encontrados nos detalhes da descoberta. As identidades são definidas pelo elemento CloudTrail UserIdentity e os valores possíveis são`Root`:`IAMUser`,,, `AssumedRole` `FederatedUserAWSAccount`, ou. `AWSService`

Além dos detalhes disponíveis para todas as GuardDuty descobertas associadas à atividade da API, AnomalousBehavioras descobertas têm detalhes adicionais que são descritos na seção a seguir. É possível visualizar esses detalhes no console e eles também estão disponíveis no JSON da descoberta.

- APIs anômalas: uma lista de solicitações de API que foram invocadas pela identidade do usuário nas proximidades da solicitação de API primária associada à descoberta. Esse painel traz ainda mais detalhes do evento da API das maneiras a seguir.
  - A primeira API listada é a API primária, que é a solicitação de API associada à atividade de maior risco observada. Essa é a API que acionou a descoberta e se correlaciona ao estágio de ataque do tipo de descoberta. Essa também é a API detalhada na seção Ação do console e no JSON da descoberta.
  - Todas as outras APIs listadas são APIs anômalas adicionais provenientes da identidade de usuário listada observada nas proximidades da API principal. Se houver apenas uma API na lista, o modelo de machine learning não identificou nenhuma solicitação de API adicional dessa identidade de usuário como anômala.
  - A lista de APIs é dividida com base no fato de uma API ter sido chamada com êxito ou se a API foi chamada sem êxito, o que significa que uma resposta de erro foi recebida. O tipo de resposta de erro recebida está listado acima de cada API chamada sem êxito. Os possíveis tipos de resposta de erro são: `access denied`, `access denied exception`, `auth failure`, `instance limit exceeded`, `invalid permission - duplicate`, `invalid permission - not found` e `operation not permitted`.
  - As APIs são categorizadas pelo serviço associado a elas.

> **Note**
>
> Para mais contexto, escolha APIs históricas para visualizar os detalhes das principais APIs, até um máximo de 20, geralmente vistas tanto para a identidade do usuário quanto

para todos os usuários da conta. As APIs são marcadas como Raras (menos de uma vez por mês), Infrequentes (algumas vezes por mês) ou Frequentes (diárias a semanais), dependendo da frequência em que são usadas na conta.

- Comportamento incomum (conta): esta seção fornece detalhes adicionais sobre o comportamento descrito para a conta. As informações rastreadas nesse painel incluem:
  - ASN Org: o ASN Org da qual a chamada de API anômala foi feita.
  - Nome de usuário: o nome do usuário que fez a chamada de API anômala.
  - Agente do usuário: o agente do usuário usado para fazer a chamada de API anômala. O agente do usuário é o método usado para fazer a chamada, como `aws-cli` ou `Botocore`.
  - Tipo de usuário: o tipo de usuário que fez a chamada de API anômala. Os valores possíveis são `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` ou `ROLE`.
  - Bucket: o nome do bucket do S3 que está sendo acessado.
- Comportamento incomum (identidade do usuário): esta seção fornece detalhes adicionais sobre o comportamento descrito para a identidade do usuário envolvida na descoberta. Quando um comportamento não é identificado como histórico, isso significa que o modelo de GuardDuty ML não viu anteriormente essa identidade de usuário fazendo essa chamada de API dessa forma durante o período de treinamento. Estes detalhes adicionais sobre a identidade do usuário estão disponíveis:
  - ASN Org: o ASN Org do qual a chamada de API anômala foi feita.
  - Agente do usuário: o agente do usuário usado para fazer a chamada de API anômala. O agente do usuário é o método usado para fazer a chamada, como `aws-cli` ou `Botocore`.
  - Bucket: o nome do bucket do S3 que está sendo acessado.
- Comportamento incomum (bucket): esta seção fornece detalhes adicionais sobre o comportamento perfilado do bucket do S3 associado à descoberta. Quando um comportamento não é identificado como histórico, isso significa que o modelo de GuardDuty ML não viu anteriormente chamadas de API feitas para esse bucket dessa forma durante o período de treinamento. As informações rastreadas nessa seção incluem:
  - ASN Org: o ASN Org do qual a chamada de API anômala foi feita.
  - Nome de usuário: o nome do usuário que fez a chamada de API anômala.
  - Agente do usuário: o agente do usuário usado para fazer a chamada de API anômala. O agente do usuário é o método usado para fazer a chamada, como `aws-cli` ou `Botocore`.
  - Tipo de usuário: o tipo de usuário que fez a chamada de API anômala. Os valores possíveis são `AWS_SERVICE`, `ASSUMED_ROLE`, `IAM_USER` ou `ROLE`.

> **Note**
>
> Para obter mais contexto sobre comportamentos históricos, selecione Comportamento histórico na seção Comportamento incomum (Conta), ID de usuário ou Bucket para ver detalhes sobre o comportamento esperado em sua conta para cada uma das seguintes categorias: Raro (menos de uma vez por mês), Infrequente (algumas vezes por mês) ou Frequente (diário ou semanal), dependendo da frequência em que são usados em sua conta.

- Comportamento incomum (banco de dados): essa seção fornece detalhes adicionais sobre o comportamento perfilado da instância do banco de dados associada à descoberta. Quando um comportamento não é identificado como histórico, isso significa que o modelo de GuardDuty ML não viu anteriormente uma tentativa de login feita nessa instância de banco de dados dessa forma durante o período de treinamento. As informações rastreadas para essa seção no painel de descoberta incluem:
  - Nome de usuário: o nome de usuário usado para fazer a tentativa anômala de login.
  - ASN Org: o ASN Org da qual a tentativa anômala de login foi feita.
  - Nome da aplicação: o nome da aplicação usada para fazer a tentativa anômala de login.
  - Nome do banco de dados: o nome da instância do banco de dados envolvida na tentativa de login anômala.

> **Note**
>
> A seção Comportamento histórico fornece mais contexto sobre os nomes de usuário, ASN Orgs, nomes de aplicações e nomes de bancos de dados observados anteriormente para o banco de dados associado. Cada valor exclusivo possui uma contagem associada que representa o número de vezes que esse valor foi observado em um evento de login bem-sucedido.

- Comportamento incomum (cluster do Kubernetes da conta, namespace do Kubernetes e nome de usuário do Kubernetes): essa seção fornece mais detalhes sobre o comportamento do perfil do cluster e do namespace do Kubernetes associado à descoberta. Quando um comportamento não é identificado como histórico, isso significa que o modelo de GuardDuty ML não observou anteriormente essa conta, cluster, namespace ou nome de usuário dessa forma. As informações rastreadas para essa seção no painel de descoberta incluem:

- Nome de usuário: o usuário que chamou a API do Kubernetes associada à descoberta.
- Nome do usuário personificado: o usuário que está sendo personificado por `username`.
- Namespace: o namespace do Kubernetes dentro do cluster Amazon EKS em que a ação ocorreu.
- Agente do usuário: o agente do usuário associado à chamada de API do Kubernetes. O agente do usuário é o método usado para fazer a chamada, como `kubectl`.
- API: a API do Kubernetes chamada pelo `username` dentro do cluster do Amazon EKS.
- Informações de ASN: as informações de ASN, como organização e ISP, associadas ao endereço IP do usuário que está fazendo essa chamada.
- Dia da semana: o dia da semana em que a chamada de API do Kubernetes foi feita.
- Permissão[1]: o verbo e o recurso do Kubernetes que estão sendo verificados quanto ao acesso para indicar se o `username` pode ou não usar a API do Kubernetes.
- Nome da conta de serviço[1]: a conta de serviço associada à workload do Kubernetes que fornece uma identidade à workload.
- Registro[1]: o registro do contêiner associado à imagem do contêiner que é implantada na workload do Kubernetes.
- Imagem[1]: a imagem do contêiner, sem as tags e o resumo associados, que é implantada na workload do Kubernetes.
- Configuração de prefixo de imagem[1]: o prefixo da imagem com o contêiner e a configuração de segurança da workload habilitados, como `hostNetwork` ou `privileged`, para o contêiner que usa a imagem.
- Nome do assunto[1]: os assuntos, como um `user`, `group` ou `serviceAccountName` que estão vinculados a uma função de referência em um `RoleBinding` ou `ClusterRoleBinding`.
- Nome da função[1]: o nome da função envolvida na criação ou modificação das funções ou da API `roleBinding`.

Anomalias com base em volume do S3

Esta seção detalha as informações contextuais relacionadas a anomalias baseadas em volume do S3. A descoberta baseada em volume (Exfiltration:S3/AnomalousBehavior) monitora números incomuns de chamadas de API do S3 feitas aos buckets do S3 pelos usuários, indicando uma possível exfiltração de dados. As chamadas de API do S3 a seguir são monitoradas em relação à detecção de anomalias com base em volume.

- `GetObject`
- `CopyObject.Read`
- `SelectObjectContent`

As métricas a seguir ajudariam a criar uma linha de base do comportamento normal quando uma entidade do IAM acessa um bucket do S3. Para detectar a exfiltração de dados, a descoberta de detecção de anomalias com base em volume avalia todas as atividades em relação à linha de base comportamental usual. Selecione Comportamento histórico nas seções Comportamento incomum (identidade do usuário), Volume observado (identidade do usuário) e Volume observado (bucket) para visualizar as seguintes métricas, respectivamente.

- Número de chamadas da API `s3-api-name` invocadas pelo usuário do IAM ou pelo perfil do IAM (depende de qual deles foi emitido) associados ao bucket do S3 afetado nas últimas 24 horas.
- Número de chamadas da API `s3-api-name` invocadas pelo usuário do IAM ou pelo perfil do IAM (depende de qual deles foi emitido) associados a todos os buckets do S3 nas últimas 24 horas.
- Número de chamadas da API `s3-api-name` em todos os usuários ou perfis do IAM (depende de qual deles foi emitido) associados ao bucket do S3 afetado nas últimas 24 horas.

Anomalias baseadas na atividade de login do RDS

Esta seção detalha a contagem de tentativas de login realizadas pelo agente incomum e é agrupada pelo resultado das tentativas de login. Os Tipos de descoberta do RDS Protection identificam comportamentos anômalos monitorando os eventos de login em busca de padrões incomuns de `successfulLoginCount`, `failedLoginCount` e `incompleteConnectionCount`.

- successfulLoginCount— Esse contador representa a soma das conexões bem-sucedidas (combinação correta de atributos de login) feitas na instância do banco de dados pelo ator incomum. Os atributos de login incluem o nome de usuário, a senha e o nome do banco de dados.
- failedLoginCount— Esse contador representa a soma das tentativas de login malsucedidas feitas para estabelecer uma conexão com a instância do banco de dados. Isso indica que um ou mais atributos da combinação de login, como o nome de usuário, a senha ou o nome do banco de dados, estavam incorretos.
- incompleteConnectionCount— Esse contador representa o número de tentativas de conexão que não podem ser classificadas como bem-sucedidas ou malsucedidas. Essas conexões são encerradas antes que o banco de dados forneça uma resposta. Por exemplo, verificação de portas em que a porta do banco de dados está conectada, mas nenhuma informação é enviada ao banco

de dados, ou a conexão foi interrompida antes que o login fosse concluído em uma tentativa bem-sucedida ou malsucedida.

Formato de busca do GuardDuty

Quando o GuardDuty detecta comportamento suspeito ou inesperado no seu ambiente da AWS, ele gera uma descoberta. Uma descoberta é uma notificação que contém os detalhes sobre um possível problema de segurança que o GuardDuty descobre. Os detalhes da descoberta incluem informações sobre o que aconteceu, quais recursos da AWS estavam envolvidos nas atividades suspeitas, quando essa atividade ocorreu e outras informações.

Uma das informações mais úteis nos detalhes de descoberta é um tipo de descoberta. O objetivo do tipo de descoberta é fornecer uma descrição concisa e legível do possível problema de segurança. Por exemplo, o tipo de descoberta Recon:EC2/PortProbeUnprotectedPort do GuardDuty informa a você rapidamente que, em algum lugar do seu ambiente da AWS, uma instância do EC2 tem uma porta desprotegida que está sendo testada por um possível invasor.

O GuardDuty usa o seguinte formato para nomear os vários tipos de descoberta que ele gera:

Propósito da ameaça: Tipo de recurso afetado/Nome da família da ameaça. Mecanismo de detecção! Artifact

Cada parte desse formato representa um aspecto de um tipo de descoberta. Esses aspectos têm as seguintes explicações:

- ThreatPurpose: descreve o objetivo principal de uma ameaça, um tipo de ataque ou uma fase de um ataque potencial. Consulte a seção a seguir para obter uma lista completa das finalidades de ameaças do GuardDuty.
- ResourceTypeAffected: descreve qual tipo de recurso da AWS é identificado nessa descoberta como o alvo potencial de um adversário. Atualmente, o GuardDuty pode gerar descobertas para recursos do EC2, S3, IAM e EKS.
- ThreatFamilyName: descreve a ameaça geral ou possível atividade maliciosa que o GuardDuty está detectando. Por exemplo, um valor de NetworkPortUnusual indica que uma instância do EC2 identificada na descoberta do GuardDuty não tem histórico prévio de comunicações em uma determinada porta remota que também é identificada na descoberta.
- DetectionMechanism - descreve o método pelo qual o GuardDuty detectou a descoberta. Isso pode ser usado para indicar uma variação em um tipo de descoberta comum ou uma descoberta

que o GuardDuty usou um mecanismo específico para detectar. Por exemplo, Backdoor:ec2/DenialOfService.tcp indica que a negação de serviço (DoS) foi detectada por TCP. A variante do UDP é Backdoor:EC2/DenialOfService.Udp.

Um valor de .Custom indica que o GuardDuty detectou a descoberta com base em suas listas de ameaças personalizadas, enquanto .Reputation indica que o GuardDuty detectou a descoberta usando um modelo de pontuação de reputação de domínio.

- Artifact – descreve um recurso específico que pertence a uma ferramenta usada no ataque. Por exemplo, DNS no tipo de descoberta CryptoCurrency:EC2/BitcoinTool.B!DNS indica que uma instância do EC2 está se comunicando com um domínio conhecido relacionado a Bitcoin.

OBJETIVO DA AMEAÇA

No GuardDuty, uma finalidade de ameaça descreve a finalidade principal de uma ameaça, um tipo de ataque ou um estágio de um possível ataque. Por exemplo, alguns propósitos de ameaça, como o Backdoor, indicam um tipo de ataque. No entanto, alguns propósitos de ameaça, como o Impact, estão alinhados às táticas do MITRE ATT&CK. As táticas do MITRE ATT&CK indicam diferentes fases no ciclo de ataque de um adversário. Na versão atual do , o ThreatPurpose pode ter os seguintes valores:

Backdoor

Esse valor indica que um adversário comprometeu um recurso da AWS e o alterou de modo que ele seja capaz de entrar em contato com o servidor de comando e controle (C&C) local para receber instruções adicionais para atividades maliciosas.

Comportamento

Esse valor indica que o GuardDuty detectou atividade ou padrões de atividade que são diferentes da linha de base estabelecida para os recursos da AWS envolvidos.

Acesso à credencial

Esse valor indica que o GuardDuty detectou padrões de atividade que um adversário pode usar para roubar credenciais, como IDs de contas ou senhas, do seu ambiente. O propósito dessa ameaça é baseado nas táticas do MITRE ATT&CK

Criptomoedas

Esse valor indica que o GuardDuty detectou que AWS um recurso em seu ambiente está hospedando software associado a criptomoedas (por exemplo, Bitcoin).

Evasão de defesa

Esse valor indica que o GuardDuty detectou atividades ou padrões de atividade que um adversário pode usar para evitar a detecção ao se infiltrar em seu ambiente. O propósito dessa ameaça é baseado nas táticas do MITRE ATT&CK

Descoberta do

Esse valor indica que o GuardDuty detectou atividades ou padrões de atividade que um adversário pode usar para expandir seu conhecimento sobre seus sistemas e redes internas. Esse propósito de ameaça é baseado nas táticas do MITRE ATT&CK.

Execução

Esse valor indica que o GuardDuty detectou que um adversário pode tentar executar um código malicioso para explorar a rede ou roubar dados. Esse propósito de ameaça é baseado nas táticas do MITRE ATT&CK.

Exfiltração

Esse valor indica que o GuardDuty detectou atividades ou padrões de atividade que um adversário pode usar ao tentar roubar dados da sua rede. Esse propósito de ameaça é baseado nas táticas do MITRE ATT&CK.

Impacto

Esse valor indica que o GuardDuty detectou atividades ou padrões de atividade que sugerem que um adversário está tentando manipular, interromper ou destruir seus sistemas e dados. O propósito dessa ameaça é baseado nas táticas do MITRE ATT&CK

Acesso inicial

O propósito dessa ameaça é baseado nas táticas do MITRE ATT&CK

PenTest

Às vezes, os proprietários de recursos da AWS ou seus representantes autorizados executam intencionalmente testes em aplicativos da AWS para encontrar vulnerabilidades, como grupos de segurança abertos ou chaves de acesso excessivamente permissivas. Esses testes de penetração são feitos na tenthabilita de identificar e bloquear recursos vulneráveis antes que eles sejam descobertos por invasores. No entanto, algumas das ferramentas usadas por testadores de penetração autorizados estão disponíveis gratuitamente e podem ser usadas por usuários não autorizados ou invasores para executar testes de sondagem. Embora o GuardDuty não possa identificar a verdadeira finalidade por trás dessa atividade, o valor do Teste de penetração indica que o GuardDuty está detectando essa atividade e que ela é semelhante à atividade gerada por

ferramentas de teste de penetração conhecidas e isso deve indicar sondagem mal-intencionada de sua rede.

Persistência

Esse valor indica que o GuardDuty detectou atividades ou padrões de atividade que um adversário pode usar para tentar manter o acesso aos seus sistemas, mesmo que sua rota de acesso inicial seja cortada. Por exemplo, isso pode incluir a criação de um novo usuário do IAM após obter acesso por meio das credenciais comprometidas de um usuário existente. Quando as credenciais do usuário existente forem excluídas, o adversário manterá o acesso ao novo usuário que não foi detectado como parte do evento original. Esse propósito de ameaça é baseado nas táticas do MITRE ATT&CK.

Política

Esse valor indica que sua conta da Conta da AWS está exibindo um comportamento que viola as melhores práticas de segurança recomendadas.

PrivilegeEscalation

Esse valor informa que o principal envolvido em seu AWS ambiente está exibindo um comportamento que um adversário pode usar para obter permissões de nível superior para sua rede. Esse propósito de ameaça é baseado nas táticas do MITRE ATT&CK.

Recon

Esse valor indica que o GuardDuty detectou atividades ou padrões de atividade que um adversário pode usar ao realizar o reconhecimento de sua rede para determinar como ele pode ampliar seu acesso ou utilizar seus recursos. Por exemplo, essa atividade pode incluir a análise de vulnerabilidades em seu AWS ambiente examinando portas, listando usuários, tabelas de banco de dados e assim por diante.

Stealth

Esse valor indica que um adversário está habilitamente tentando esconder suas ações. Por exemplo, eles podem usar um servidor proxy anônimo, tornando extremamente difícil avaliar a verdadeira natureza da atividade.

Trojan

Esse valor indica que um ataque está usando programas de Trojan que realizam atividades mal-intencionadas silenciosas. Às vezes, esse software assume a aparência de um programa legítimo. Às vezes, os usuários executam esse software acidentalmente. Outras vezes, esse software pode ser executado automaticamente por meio da exploração de uma vulnerabilidade.

UnauthorizedAccess

Esse valor indica que o GuardDuty está detectando atividade suspeita ou um padrão de atividade suspeita realizada por um indivíduo não autorizado.

Gerando resultados de amostras em GuardDuty

Você pode gerar amostras de descobertas com GuardDuty a Amazon para ajudá-lo a visualizar e entender os vários tipos de descobertas que GuardDuty podem gerar. Ao gerar resultados de amostra, GuardDuty preenche sua lista de descobertas atual com uma descoberta de amostra para cada tipo de descoberta compatível.

As amostras geradas são aproximações preenchidas com valores de espaço reservado. Essas amostras podem parecer diferentes das descobertas reais do seu ambiente, mas você pode usá-las para testar várias configurações GuardDuty, como seus CloudWatch eventos ou filtros. Para obter uma lista dos valores disponíveis para encontrar, os tipos estão listados na tabela Tipos de descoberta.

Para gerar algumas descobertas comuns com base em atividades simuladas dentro do ambiente, consulte Geração automática de GuardDuty descobertas comuns a seguir.

Gerando amostras de descobertas por meio do GuardDuty console ou da API

Selecione seu método de acesso preferido para gerar descobertas de amostra.

> **Note**
>
> O método do console gera um de cada tipo de descoberta. As descobertas de amostra únicas só podem ser geradas por meio da API.

Console

Use o procedimento a seguir para gerar descobertas de amostra. Esse processo gera uma amostra de descoberta para cada tipo de GuardDuty descoberta.

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

2. No painel de navegação, selecione Configurações.
3. Na página Settings, em Sample findings, escolha Generate sample findings.
4. No painel de navegação, selecione Descobertas. As descoberta de amostra são exibidas na página Descobertas atuais com o prefixo [SAMPLE].

API/CLI

Você pode gerar uma única amostra de descoberta que corresponda a qualquer um dos tipos de GuardDuty descoberta por meio da CreateSampleFindingsAPI. Os valores disponíveis para os tipos de descoberta estão listados na Tipos de descoberta tabela.

Isso é útil para testar regras de CloudWatch eventos ou automação com base nas descobertas. O exemplo a seguir mostra como gerar uma descoberta de amostra única do tipo `Backdoor:EC2/DenialOfService.Tcp` usando a AWS CLI.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty create-sample-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --finding-types Backdoor:EC2/DenialOfService.Tcp
```

O título das descobertas de amostra geradas por meio de algum desses métodos sempre começa com [SAMPLE] no console. As descobertas de amostra têm um valor de `"sample": true` na seção additionalInfo dos detalhes do JSON de descoberta.

Geração automática de GuardDuty descobertas comuns

Você pode usar os scripts a seguir para gerar automaticamente várias GuardDuty descobertas comuns. O guardduty-tester.template é usado AWS CloudFormation para criar um ambiente isolado com um bastion host, uma instância testadora do Amazon EC2 que você pode acessar por meio de SSH e duas instâncias EC2 de destino. Em seguida, você pode executar o guardduty_tester.sh para iniciar uma interação entre a instância do EC2 do testador, a instância do Windows EC2 de destino e a instância do EC2 do Linux de destino, para simular cinco tipos de ataques comuns que GuardDuty podem detectar e notificar você com as descobertas geradas.

1. Como pré-requisito, você deve habilitar GuardDuty na conta e na região em que deseja executar guardduty-tester.template e guardduty_tester.sh. Para obter mais informações sobre como habilitar GuardDuty, consulteComeçando com GuardDuty.

Também é necessário gerar um novo ou usar um par de chaves do EC2 em cada região na qual você deseja executar esses scripts. Esse par de chaves do EC2 é usado como um parâmetro no script guardduty-tester.template que você usa para criar uma nova pilha. CloudFormation Para obter mais informações sobre como gerar pares de chaves, consulte Pares de chaves do Amazon EC2.

2. Crie uma nova CloudFormation pilha usando guardduty-tester.template. Para obter instruções sobre como criar uma pilha, consulte Como criar uma pilha. Antes de executar guardduty-tester.template, modifique-o com valores para os seguintes parâmetros: nome da pilha, para identificar sua nova pilha; zona de disponibilidade na qual você deseja executar a pilha; e par de chaves que pode ser usado para iniciar as instâncias do EC2. Em seguida, você pode usar a chave privada correspondente ao SSH nas instâncias do EC2.

   O guardduty-tester.template leva cerca de 10 minutos para ser executado e concluído. Ele cria seu ambiente e copia guardduty_tester.sh na sua instância do EC2 testadora.

3. No AWS CloudFormation console, escolha a caixa de seleção ao lado da nova AWS CloudFormation pilha em execução. No conjunto de guias exibidas, selecione a guia Output (Saída). Observe os endereços IP atribuídos ao bastion host e à instância do EC2 testadora. Você precisa desses dois endereços IP para se conectar à instância do EC2 testadora.

4. Crie a entrada a seguir no arquivo ~/.ssh/config para fazer login na sua instância pelo bastion host.

```
Host bastion
        HostName {Elastic IP Address of Bastion}
        User ec2-user
        IdentityFile ~/.ssh/{your-ssh-key.pem}
Host tester
        ForwardAgent yes
        HostName {Local IP Address of RedTeam Instance}
        User ec2-user
        IdentityFile ~/.ssh/{your-ssh-key.pem}
        ProxyCommand ssh bastion nc %h %p
        ServerAliveInterval 240
```

Agora, é possível chamar $ ssh tester para fazer login na instância do EC2 de destino. Para obter mais informações sobre como configurar e se conectar a instâncias do EC2 por meio de bastion hosts, consulte https://aws.amazon.com/blogs/security/ securely-connect-to-linux - - instances-running-in-a/. private-amazon-vpc

5. Depois de se conectar à instância do EC2 testador, execute o guardduty_tester.sh para iniciar a interação entre seu testador e as instâncias EC2 de destino, simular ataques e gerar descobertas. GuardDuty

Níveis de severidade GuardDuty das descobertas

Cada GuardDuty descoberta tem um nível de gravidade e um valor atribuídos que refletem o risco potencial que a descoberta pode ter para sua rede, conforme determinado por nossos engenheiros de segurança. O valor da gravidade pode estar entre 1,0 e 8,9, com valores mais altos indicando maior risco de segurança. Para ajudá-lo a determinar uma resposta a um possível problema de segurança destacado por uma descoberta, GuardDuty divide esse intervalo em níveis de severidade altos, médios e baixos.

> **Note**
>
> Os valores 0 e de 9.0 a 10.0 estão reservados para uso futuro.

A seguir estão os níveis e valores de severidade atualmente definidos para os GuardDuty resultados, bem como recomendações gerais para cada um:

Nível de gravidade	Intervalo de valores
Alto	7,0 - 8,9
Um nível de gravidade alto indica que o recurso (uma instância do EC2 ou um conjunto de credenciais de usuários do IAM) está comprometido e é usado ativamente para fins não autorizados. Recomendamos que você trate todos os problemas de segurança das descobertas de gravidade alta como prioridade e tome medidas de correção imediatas para impedir o uso não autorizado de seus recursos. Por exemplo, limpe sua instância do EC2 ou encerre-a, ou mude as credenciais do IAM. Consulte Etapas de correção para obter mais detalhes.	
Médio	4,0 - 6,9

Nível de gravidade	Intervalo de valores
Um nível de gravidade médio indica atividade suspeita que se desvia do comportamento normalmente observado e, dependendo do caso de uso, pode indicar o comprometimento de recursos. Recomendamos que você investigue o recurso implicado o mais cedo possível. As etapas de correção variam de acordo com o recurso e a família da descoberta, mas, em geral, você deve confirmar se a atividade está autorizada e é consistente com o caso de uso. Se você não conseguir identificar a causa ou confirmar se a atividade foi autorizada, considere o recurso como comprometido e siga as Etapas de correção para proteger o recurso. Veja alguns itens a serem considerados ao analisar uma descoberta de nível médio: • Verifique se um usuário autorizado instalou um novo software que alterou o comportamento de um recurso (por exemplo, permitido tráfego superior ao normal ou comunicação habilitada em uma nova porta). • Verifique se um usuário autorizado alterou as configurações do painel de controle, por exemplo, modificou uma configuração de grupo de segurança. • Execute uma verificação antivírus no recurso implicado para detectar software não autorizado. • Verifique as permissões associadas ao perfil, usuário, grupo ou conjunto de credenciais afetados do IAM. Pode ser necessário alterá-las.	
Baixo	1,0 - 3,9
Um nível de gravidade baixo indica tentativa de atividade suspeita que não comprometeu sua rede. Por exemplo, uma verificação de porta ou tentativa de intrusão malsucedida. Não há nenhuma ação recomendada imediata, mas vale a pena anotar essas informações, pois isso pode indicar que alguém está procurando pontos fracos em sua rede.	

GuardDuty encontrando agregação

Todas as descobertas são dinâmicas, o que significa que, se GuardDuty detectar uma nova atividade relacionada ao mesmo problema de segurança, ela atualizará a descoberta original com as novas informações, em vez de gerar uma nova descoberta. Esse comportamento permite que você

identifique problemas em andamento sem precisar examinar relatórios similares, e reduz o ruído geral de problemas de segurança dos quais já está ciente.

Por exemplo, para uma descoberta `UnauthorizedAccess:EC2/SSHBruteForce`, múltiplas tentativas de acesso à sua instância serão agregadas ao mesmo ID da descoberta, aumentando o número de co1ntagem nos detalhes da descoberta. Isso ocorre porque essa descoberta representa um único problema de segurança com a instância, indicando que a porta SSH da instância não está adequadamente protegida contra esse tipo de atividade. No entanto, se GuardDuty detectar atividade de acesso SSH direcionada a uma nova instância em seu ambiente, ela criará uma nova descoberta com um ID de descoberta exclusivo para alertá-lo sobre o fato de que há um problema de segurança associado ao novo recurso.

Quando uma descoberta é agregada, ela é atualizada com as informações da última ocorrência dessa atividade. Quando uma descoberta é agregada, ela é atualizada com as informações da ocorrência mais recente dessa atividade, o que significa que, no exemplo acima, se sua instância for alvo de uma tentativa de força bruta de um novo ator, os detalhes da descoberta serão atualizados para refletir o IP remoto da fonte mais recente e as informações mais antigas serão substituídas. Informações completas sobre tentativas de atividades individuais ainda estarão disponíveis em seus registros de fluxo CloudTrail ou no VPC Flow Logs.

Os critérios que alertam GuardDuty para gerar uma nova descoberta em vez de agregar uma existente dependem do tipo de descoberta. Os critérios de agregação para cada tipo de descoberta são determinados por nossos engenheiros de segurança para fornecer a melhor visão geral de diferentes problemas de segurança em sua conta.

Localizando e analisando descobertas GuardDuty

Use o procedimento a seguir para visualizar e analisar suas GuardDuty descobertas.

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. Escolha Descobertas e selecione uma descoberta específica para visualizar os detalhes.

   Os detalhes de cada descoberta serão diferentes, de acordo com o tipo de descoberta, os recursos envolvidos e a natureza da atividade. Para obter mais informações sobre campos de descobertas disponíveis, consulte Detalhes da descoberta.
3. (Opcional) Se você deseja arquivar uma descoberta, selecione-a na lista de descobertas e escolha o menu Ações. Depois escolha Arquivar.

As descobertas arquivadas podem ser visualizadas ao escolher Arquivadas no menu suspenso Atual.

Atualmente, os GuardDuty usuários das contas GuardDuty dos membros não podem arquivar as descobertas.

> **Important**
>
> Se você arquivar uma descoberta manualmente usando o procedimento acima, todas as ocorrências subsequentes dessa descoberta (geradas após a conclusão do arquivamento) serão adicionadas à lista das suas descobertas atuais. Para não ver essa descoberta na sua lista atual, você pode autoarquivá-la. Para ter mais informações, consulte Regras de supressão.

4. (Opcional) Para fazer download de uma descoberta, selecione-a na lista de descobertas e escolha o menu Ações. Depois escolha Exportar. Quando você exportar uma descoberta, você poderá visualizar o documento JSON completo.

> **Note**
>
> Em alguns casos, GuardDuty fica ciente de que certas descobertas são falsos positivos depois de terem sido geradas. GuardDuty fornece um campo Confiança no JSON da descoberta e define seu valor como zero. GuardDuty Dessa forma, você sabe que pode ignorar essas descobertas com segurança.

Tipos de descoberta

Para obter informações sobre mudanças importantes nos tipos de GuardDuty descoberta, incluindo tipos de descoberta recém-adicionados ou retirados, consulteHistórico de documentos da Amazon GuardDuty.

Para obter informações sobre os tipos de busca que agora estão desabilitados, consulte Tipos de descoberta desabilitados.

GuardDuty Tipos de descoberta do EC2

As descobertas a seguir são específicas dos recursos do Amazon EC2 e sempre têm um tipo de recurso `Instance`. A gravidade e os detalhes das descobertas serão diferentes com base na função de recurso, que indicará se a instância do EC2 foi alvo de atividade suspeita ou o agente que executou a atividade.

As descobertas listadas aqui incluem as fontes de dados e os modelos usados para gerar esse tipo de descoberta. Para obter mais informações sobre modelos e fontes de dados, consulte Fontes de dados fundamentais.

> **Note**
>
> Os detalhes da instância podem estar ausentes em algumas descobertas do EC2 ela já tiver sido encerrada ou se a chamada de API subjacente fizer parte de uma chamada de API entre regiões originada de uma instância do EC2 em uma região diferente.

Para todas as descobertas do EC2, recomenda-se examinar o recurso em questão para determinar se ele está se comportando da maneira esperada. Se a atividade for autorizada, você poderá usar regras de supressão ou listas de IP confiáveis para evitar notificações de falsos positivos para esse recurso. Se a atividade for inesperada, a melhor prática de segurança será presumir que a instância foi comprometida e executar as ações detalhadas em Correção de uma instância potencialmente comprometida do Amazon EC2.

Tópicos

- Backdoor:EC2/C&CActivity.B
- Backdoor:EC2/C&CActivity.B!DNS

- Backdoor:EC2/DenialOfService.Dns
- Backdoor:EC2/DenialOfService.Tcp
- Backdoor:EC2/DenialOfService.Udp
- Backdoor:EC2/DenialOfService.UdpOnTcpPorts
- Backdoor:EC2/DenialOfService.UnusualProtocol
- Backdoor:EC2/Spambot
- Behavior:EC2/NetworkPortUnusual
- Behavior:EC2/TrafficVolumeUnusual
- CryptoCurrency:EC2/BitcoinTool.B
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- DefenseEvasion:EC2/UnusualDNSResolver
- DefenseEvasion:EC2/UnusualDoHActivity
- DefenseEvasion:EC2/UnusualDoTActivity
- Impact:EC2/AbusedDomainRequest.Reputation
- Impact:EC2/BitcoinDomainRequest.Reputation
- Impact:EC2/MaliciousDomainRequest.Reputation
- Impact:EC2/PortSweep
- Impact:EC2/SuspiciousDomainRequest.Reputation
- Impact:EC2/WinRMBruteForce
- Recon:EC2/PortProbeEMRUnprotectedPort
- Recon:EC2/PortProbeUnprotectedPort
- Recon:EC2/Portscan
- Trojan:EC2/BlackholeTraffic
- Trojan:EC2/BlackholeTraffic!DNS
- Trojan:EC2/DGADomainRequest.B
- Trojan:EC2/DGADomainRequest.C!DNS
- Trojan:EC2/DNSDataExfiltration
- Trojan:EC2/DriveBySourceTraffic!DNS
- Trojan:EC2/DropPoint
- Trojan:EC2/DropPoint!DNS

- Trojan:EC2/PhishingDomainRequest!DNS
- UnauthorizedAccess:EC2/MaliciousIPCaller.Custom
- UnauthorizedAccess:EC2/MetadataDNSRebind
- UnauthorizedAccess:EC2/RDPBruteForce
- UnauthorizedAccess:EC2/SSHBruteForce
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay

Backdoor:EC2/C&CActivity.B

A instância do EC2 está consultando um IP associado a um servidor de controle e comando conhecido.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância listada em seu ambiente da AWS está consultando um IP associado a um servidor de comando e controle (C&C) conhecido. A instância listada pode estar comprometida. Os servidores de comando e controle são computadores que enviam comandos para membros de um botnet.

Um botnet é uma coleção de dispositivos conectados à Internet, que podem incluir PCs, servidores, dispositivos móveis e dispositivos de Internet das Coisas, infectados e controlados por um tipo comum de malware. Os botnets são frequentemente usados para distribuir malwares e coletar informações inapropriadas, como números de cartão de crédito. Dependendo da finalidade e da estrutura do botnet, o servidor C&C também pode emitir comandos para iniciar um ataque de negação distribuída de serviço DDoS.

> **Note**
>
> Se o IP consultado estiver relacionado ao log4j, os campos da descoberta associada incluirão estes valores:
>
> - Serviço. Informações adicionais. threatListName = Amazon

- service.additionalInfo.threatName = relacionado ao Log4j

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Backdoor:EC2/C&CActivity.B!DNS

A instância do EC2 está consultando um nome de domínio associado a um servidor de controle e comando conhecido.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância listada em seu ambiente da AWS está consultando um nome de domínio associado a um servidor de comando e controle (C&C) conhecido. A instância listada pode estar comprometida. Os servidores de comando e controle são computadores que enviam comandos para membros de um botnet.

Um botnet é uma coleção de dispositivos conectados à Internet, que podem incluir PCs, servidores, dispositivos móveis e dispositivos de Internet das Coisas, infectados e controlados por um tipo comum de malware. Os botnets são frequentemente usados para distribuir malwares e coletar informações inapropriadas, como números de cartão de crédito. Dependendo da finalidade e da estrutura do botnet, o servidor C&C também pode emitir comandos para iniciar um ataque de negação distribuída de serviço DDoS.

> **Note**
>
> Se o nome de domínio consultado estiver relacionado ao log4j, os campos da descoberta associada incluirão os seguintes valores:
>
> - Serviço. Informações adicionais. threatListName = Amazon
> - service.additionalInfo.threatName = relacionado ao Log4j

> **Note**
>
> Para testar como GuardDuty gera esse tipo de descoberta, você pode fazer uma solicitação de DNS da sua instância (usando `dig` para Linux ou `nslookup` Windows) em um domínio `guarddutyc2activityb.com` de teste.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Backdoor:EC2/DenialOfService.Dns

Uma instância do EC2 está se comportando de uma forma que pode indicar que está sendo usada para executar um ataque de negação de serviço (DoS) usando o protocolo DNS.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está gerando um grande volume de tráfego DNS de saída. Isso pode indicar que a instância listada está comprometida e está sendo usada para realizar ataques denial-of-service (DoS) usando o protocolo DNS.

> **Note**
>
> Essa descoberta detecta os ataques somente contra endereços IP publicamente roteáveis, que são alvos primários de ataques.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Backdoor:EC2/DenialOfService.Tcp

Uma instância do EC2 está se comportando de uma forma que indica que ela está sendo usada para executar um ataque de negação de serviço (DoS – Denial of Service) usando o protocolo TCP.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está gerando um grande volume de tráfego TCP de saída. Isso pode indicar que a instância está comprometida e sendo usada para realizar ataques denial-of-service (DoS) usando o protocolo TCP.

> **Note**
>
> Essa descoberta detecta os ataques somente contra endereços IP publicamente roteáveis, que são alvos primários de ataques.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Backdoor:EC2/DenialOfService.Udp

Uma instância do EC2 está se comportando de uma forma que indica que ela está sendo usada para executar um ataque de negação de serviço (DoS) usando o protocolo UDP.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está gerando um grande volume de tráfego UDP de saída. Isso pode indicar que a instância listada está comprometida e está sendo usada para realizar ataques denial-of-service (DoS) usando o protocolo UDP.

> **Note**
>
> Essa descoberta detecta os ataques somente contra endereços IP publicamente roteáveis, que são alvos primários de ataques.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Backdoor:EC2/DenialOfService.UdpOnTcpPorts

Uma instância do EC2 está se comportando de uma forma que pode indicar que está sendo usada para executar um ataque de negação de serviço (DoS) usando o protocolo UDP em uma porta TCP.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está gerando um grande volume de tráfego UDP de saída direcionado a uma porta que normalmente é usada para comunicação TCP. Isso pode indicar que a instância listada está comprometida e está sendo usada para realizar ataques denial-of-service (DoS) usando o protocolo UDP em uma porta TCP.

> **Note**
>
> Essa descoberta detecta os ataques somente contra endereços IP publicamente roteáveis, que são alvos primários de ataques.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Backdoor:EC2/DenialOfService.UnusualProtocol

Uma instância do EC2 está se comportando de uma forma que pode indicar que está sendo usada para executar um ataque de negação de serviço (DoS) usando um protocolo incomum.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada no seu ambiente da AWS está gerando um grande volume de tráfego de saída de um tipo de protocolo incomum que não é normalmente usado por instâncias do EC2, como Internet Group Management Protocol. Isso pode indicar que a instância está comprometida e está sendo usada para realizar ataques denial-of-service (DoS) usando um protocolo incomum. Essa descoberta detecta os ataques somente contra endereços IP publicamente roteáveis, que são alvos primários de ataques.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Backdoor:EC2/Spambot

A instância do EC2 está exibindo um comportamento incomum ao se comunicar com um host remoto na porta 25.

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está se comunicando com um host remoto na porta 25. Esse comportamento é incomum, pois essa instância do EC2 não possui histórico prévio de comunicações com a porta 25. A porta 25 é tradicionalmente

usada por servidores de e-mail para comunicações SMTP. Essa descoberta indica que a instância do EC2 pode estar comprometida para uso no envio de spam.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Behavior:EC2/NetworkPortUnusual

Uma instância do EC2 está se comunicando com um host remoto em uma porta de servidor incomum.

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está se comportando de uma forma que se desvia da linha de base estabelecida. Essa instância do EC2 não possui histórico prévio de comunicações com essa porta remota.

> **Note**
>
> Se a instância do EC2 se comunicar na porta 389 ou na porta 1389, a gravidade da descoberta associada será modificada para Alta e os campos de descoberta incluirão o seguinte valor:
>
> - service.additionalInfo.context = possível retorno de chamada ao log4j

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Behavior:EC2/TrafficVolumeUnusual

A instância do EC2 está gerando quantidades grandes incomuns de tráfego de rede para um host remoto.

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está se comportando de uma forma que se desvia da linha de base estabelecida. Esta instância do EC2 não tem histórico prévio de enviar tráfego assim para esse host remoto.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

CryptoCurrency:EC2/BitcoinTool.B

Uma instância do EC2 está consultando um endereço IP associado à atividade relacionada à criptomoeda.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está consultando um endereço IP associado ao Bitcoin ou a outras atividades relacionadas a criptomoedas. O Bitcoin é uma criptomoeda mundial e um sistema de pagamento digital que pode ser trocado por outras moedas, produtos e serviços. O Bitcoin é uma recompensa pela mineração de bitcoins e é muito procurado por agentes de ameaças.

Recomendações de correção:

Se você usar essa instância do EC2 para minerar ou gerenciar criptomoeda ou se essa instância estiver envolvida de outra forma na atividade de blockchain, essa descoberta poderia representar a atividade esperada para o ambiente. Se esse for o caso em seu ambiente da AWS, recomendamos configurar uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `CryptoCurrency:EC2/BitcoinTool.B`. O segundo critério de filtro deve ser o ID de instância da instância envolvida na atividade de blockchain. Para saber mais sobre a criação de regras de supressão, consulte Regras de supressão.

Se essa atividade for inesperada, sua instância provavelmente está comprometida. Consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

CryptoCurrency:EC2/BitcoinTool.B!DNS

Uma instância do EC2 está consultando um nome de domínio associado à atividade relacionada à criptomoeda.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está consultando um nome de domínio associado ao Bitcoin ou a outras atividades relacionadas a criptomoedas. O Bitcoin é uma criptomoeda mundial e um sistema de pagamento digital que pode ser trocado por outras moedas, produtos e serviços. O Bitcoin é uma recompensa pela mineração de bitcoins e é muito procurado por agentes de ameaças.

Recomendações de correção:

Se você usar essa instância do EC2 para minerar ou gerenciar criptomoeda ou se essa instância estiver envolvida de outra forma na atividade de blockchain, essa descoberta poderia representar a atividade esperada para o ambiente. Se esse for o caso em seu ambiente da AWS, recomendamos configurar uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `CryptoCurrency:EC2/BitcoinTool.B!DNS`. O segundo critério de filtro deve ser o ID de instância da instância envolvida na atividade de blockchain. Para saber mais sobre a criação de regras de supressão, consulte Regras de supressão.

Se essa atividade for inesperada, sua instância provavelmente está comprometida. Consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

DefenseEvasion:EC2/UnusualDNSResolver

Uma instância do Amazon EC2 está se comunicando com um resolvedor de DNS público incomum.

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do Amazon EC2 listada em seu ambiente da AWS está se comportando de uma forma que se desvia do comportamento da linha de base. Essa instância do EC2 não tem histórico recente de comunicação com esse resolvedor de DNS público. O campo Incomum no painel de detalhes da descoberta no GuardDuty console pode fornecer informações sobre o resolvedor de DNS consultado.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

DefenseEvasion:EC2/UnusualDoHActivity

Uma instância do Amazon EC2 está executando uma comunicação incomum de DNS sobre HTTPS (DoH).

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do Amazon EC2 listada em seu ambiente da AWS está se comportando de uma forma que se desvia da linha de base estabelecida. Essa instância do EC2 não tem histórico recente de comunicações de DNS sobre HTTPS (DoH) com esse servidor público do DoH. Nos detalhes da descoberta, o campo Incomum pode fornecer informações sobre o servidor DoH consultado.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

DefenseEvasion:EC2/UnusualDoTActivity

Uma instância do Amazon EC2 está executando uma comunicação incomum de DNS sobre TLS (DoT).

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está se comportando de uma forma que se desvia da linha de base estabelecida. Essa instância do EC2 não tem histórico recente de comunicações de DNS sobre TLS (DoT) com esse servidor DoT público. No painel de detalhes da descoberta, o campo Incomum pode fornecer informações sobre o servidor DoT consultado.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Impact:EC2/AbusedDomainRequest.Reputation

Uma instância do EC2 está consultando um nome de domínio com baixa reputação associado a domínios conhecidos que permitem abusos.

Gravidade padrão: média

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância do Amazon EC2 listada em seu ambiente da AWS está consultando um nome de domínio de baixa reputação associado a domínios ou endereços IP de abuso conhecidos. Exemplos de domínios abusados são nomes de domínio de nível superior (TLDs) e nomes de domínio de segundo nível (2LDs) que fornecem registros gratuitos de subdomínios, bem como provedores de DNS dinâmicos. Os agentes de ameaças tendem a usar esses serviços para registrar domínios gratuitamente ou a baixo custo. Os domínios de baixa reputação nessa categoria também podem ser domínios expirados que se resolvem para o endereço IP estacionário de um registrador e, portanto, podem não estar mais ativas. Um IP de estacionamento é onde um registrador direciona o tráfego para domínios que não foram vinculados a nenhum serviço. É possível que a instância listada do Amazon EC2 esteja comprometida, pois os agentes de ameaças geralmente usam esses registradores ou serviços para C&C e distribuição de malware.

Os domínios de baixa reputação são baseados em um modelo de pontuação de reputação. Esse modelo avalia e classifica as características de um domínio para determinar sua probabilidade de ser mal-intencionado.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Impact:EC2/BitcoinDomainRequest.Reputation

Uma instância do EC2 está consultando um nome de domínio associado à atividade relacionada à criptomoeda.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância do Amazon EC2 listada em seu ambiente da AWS está consultando um nome de domínio de baixa reputação associado ao Bitcoin ou a outras atividades relacionadas a criptomoedas. O Bitcoin é uma criptomoeda mundial e um sistema de pagamento digital que pode ser trocado por outras moedas, produtos e serviços. O Bitcoin é uma recompensa pela mineração de bitcoins e é muito procurado por agentes de ameaças.

Os domínios de baixa reputação são baseados em um modelo de pontuação de reputação. Esse modelo avalia e classifica as características de um domínio para determinar sua probabilidade de ser mal-intencionado.

Recomendações de correção:

Se você usar essa instância do EC2 para minerar ou gerenciar criptomoeda ou se essa instância estiver envolvida de outra forma na atividade de blockchain, essa descoberta poderia representar a atividade esperada para o ambiente. Se esse for o caso em seu ambiente da AWS, recomendamos configurar uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `Impact:EC2/BitcoinDomainRequest.Reputation`. O segundo critério de filtro deve ser o ID de instância da instância envolvida na atividade de blockchain. Para saber mais sobre a criação de regras de supressão, consulte Regras de supressão.

Se essa atividade for inesperada, sua instância provavelmente está comprometida. Consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Impact:EC2/MaliciousDomainRequest.Reputation

Uma instância do EC2 está consultando um domínio de baixa reputação associado a domínios mal-intencionados conhecidos.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância do Amazon EC2 listada em seu ambiente da AWS está consultando um nome de domínio de baixa reputação associado a domínios ou endereços IP mal-intencionados conhecidos. Por exemplo, os domínios podem estar associados a um endereço IP sumidouro conhecido. Domínios sinkholed são domínios que antes eram controlados por um agente de ameaças, e as solicitações feitas a eles podem indicar que a instância está comprometida. Esses domínios também podem estar correlacionados com campanhas mal-intencionadas conhecidas ou algoritmos de geração de domínio.

Os domínios de baixa reputação são baseados em um modelo de pontuação de reputação. Esse modelo avalia e classifica as características de um domínio para determinar sua probabilidade de ser mal-intencionado.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Impact:EC2/PortSweep

Uma instância do EC2 está testando uma porta em um muitos endereços IP.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está testando uma porta em um grande número de endereços IP roteáveis publicamente. Esse tipo de atividade geralmente é usado para encontrar hospedeiros vulneráveis para serem explorados. No painel de detalhes de busca em seu GuardDuty console, somente o endereço IP remoto mais recente é exibido

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Impact:EC2/SuspiciousDomainRequest.Reputation

Uma instância do EC2 está consultando um nome de domínio com baixa reputação que é suspeito por natureza devido à sua idade ou baixa popularidade.

Gravidade padrão: baixa

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância do Amazon EC2 listada em seu ambiente da AWS está consultando um nome de domínio com baixa reputação que é suspeito de ser mal-intencionado. Foram percebidas características desse domínio que eram consistentes com domínios mal-intencionados observados anteriormente. No entanto, nosso modelo de reputação não conseguiu relacioná-lo definitivamente a uma ameaça conhecida. Esses domínios geralmente são observados recentemente ou recebem uma quantidade baixa de tráfego.

Os domínios de baixa reputação são baseados em um modelo de pontuação de reputação. Esse modelo avalia e classifica as características de um domínio para determinar sua probabilidade de ser mal-intencionado.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Impact:EC2/WinRMBruteForce

Uma instância do EC2 está executando um ataque de força bruta de saída do Gerenciamento Remoto do Windows.

Gravidade padrão: baixa*

> **Note**
>
> A gravidade dessa descoberta é baixa se a instância do EC2 foi o alvo de um ataque de força bruta. A gravidade dessa descoberta será alta se sua instância do EC2 for o agente que está sendo usado para executar o ataque de força bruta.

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está executando um ataque de força bruta do Gerenciamento Remoto do Windows (WinRM) com o objetivo de obter acesso ao serviço de Gerenciamento Remoto do Windows em sistemas baseados em Windows.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Recon:EC2/PortProbeEMRUnprotectedPort

Uma instância do EC2 tem uma porta relacionada ao EMR desprotegida que está sendo testada por um host mal-intencionado conhecido.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que uma porta confidencial relacionada ao EMR na instância EC2 listada que faz parte de um cluster em AWS seu ambiente não está bloqueada por um grupo de segurança, uma lista de controle de acesso (ACL) ou um firewall no host, como Linux IPTables. Essa descoberta

também informa que scanners conhecidos na Internet estão investigando ativamente essa porta. Portas que podem acionar essa descoberta, como a porta 8088 (porta da IU da Web do YARN), possivelmente podem ser usadas para execução de código remoto.

Recomendações de correção:

Você deve bloquear o acesso a portas abertas nos clusters pela Internet e restringir o acesso apenas a endereços IP específicos que exigem acesso a essas portas. Para obter mais informações, consulte Grupos de segurança para a clusters do EMR.

Recon:EC2/PortProbeUnprotectedPort

Uma instância do EC2 tem uma porta desprotegida que está sendo testada por um host mal-intencionado conhecido.

Gravidade padrão: baixa*

> **Note**
>
> A gravidade padrão dessa descoberta é baixa. No entanto, se a porta que está sendo testada for usada pelo Elasticsearch (9200 ou 9300), a gravidade da descoberta será alta.

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que uma porta na instância do EC2 listada em seu ambiente da AWS não está bloqueada por um grupo de segurança, uma lista de controle de acesso (ACL) ou um firewall no host, como o IPTables do Linux, e que scanners conhecidos na Internet estão sondando-a ativamente.

Se a porta desprotegida identificada for 22 ou 3389 e você estiver usando essas portas para se conectar à instância, ainda será possível limitar a exposição permitindo o acesso a essas portas somente aos endereços IP do espaço de endereços IP da rede corporativa. Para restringir o acesso à porta 22 no Linux, consulte Autorizar o tráfego de entrada para suas instâncias do Linux. Para restringir o acesso à porta 3389 no Windows, consulte Autorizar o tráfego de entrada para suas instâncias do Windows.

GuardDuty não gera essa descoberta para as portas 443 e 80.

Recomendações de correção:

Pode haver casos em que instâncias são intencionalmente expostas, por exemplo, se estão hospedando servidores web. Se esse for o caso em seu ambiente da AWS, recomendamos configurar uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `Recon:EC2/PortProbeUnprotectedPort`. O segundo critério de filtro deve corresponder à instância ou às instâncias que servem como um bastion host. É possível usar o atributo ID da imagem da instância ou o atributo de valor da Tag dependendo de quais critérios forem identificáveis com as instâncias que hospedam essas ferramentas. Para obter mais informações sobre como criar regras de supressão, consulte Regras de supressão.

Se essa atividade for inesperada, sua instância provavelmente está comprometida. Consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Recon:EC2/Portscan

Uma instância do EC2 está executando verificações de portas de saída para um host remoto.

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está envolvida em um possível ataque de varredura de porta porque está tentando se conectar a várias portas em um curto período de tempo. O objetivo de um ataque de verificação de porta é localizar portas abertas para descobrir quais serviços a máquina está executando e identificar o sistema operacional dela.

Recomendações de correção:

Essa descoberta pode ser um falso positivo quando aplicativas de avaliação de vulnerabilidade são implantados em instâncias do EC2 no ambiente, pois esses aplicativas realizam verificações de portas para alertar sobre portas abertas configuradas incorretamente. Se esse for o caso em seu ambiente da AWS, recomendamos configurar uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `Recon:EC2/Portscan`. O segundo critério de filtro

deve corresponder à instância ou às instâncias que hospedam essas ferramentas de avaliação de vulnerabilidade. É possível usar o atributo ID da imagem da instância ou o atributo de valor da Tag dependendo de quais critérios forem identificáveis com as instâncias que hospedam essas ferramentas. Para obter mais informações sobre como criar regras de supressão, consulte Regras de supressão.

Se essa atividade for inesperada, sua instância provavelmente está comprometida. Consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Trojan:EC2/BlackholeTraffic

Uma instância do EC2 está tentando se comunicar com um endereço IP de um host remoto que é um buraco negro conhecido.

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS pode estar comprometida porque está tentando se comunicar com um endereço IP de um buraco negro (ou sumidouro). Os buracos negros são locais na rede onde o tráfego de entrada ou de saída é descartado silenciosamente sem informar a fonte de que os dados não atingiram o destinatário pretendido. Um endereço IP de buraco negro especifica uma máquina host que não está sendo executada ou um endereço para o qual nenhum host foi atribuído.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Trojan:EC2/BlackholeTraffic!DNS

Uma instância do EC2 está consultando um nome de domínio que está sendo redirecionado para o endereço IP de um buraco negro.

Gravidade padrão: média

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS pode estar comprometida porque está consultando um nome de domínio que está sendo redirecionado para um endereço IP de buraco negro. Os buracos negros são locais na rede onde o tráfego de entrada ou de saída é descartado silenciosamente sem informar a fonte de que os dados não atingiram o destinatário pretendido.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Trojan:EC2/DGADomainRequest.B

Uma instância do EC2 está consultando domínios gerados por algoritmos. Esses domínios são comumente usados por malware e podem ser um indicativo de uma instância do EC2 comprometida.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância do EC2 listada no seu ambiente da AWS está tentando consultar domínios do algoritmo de geração de domínio (DGA). Sua instância do EC2 pode estar comprometida.

Os DGAs são usados para gerar uma grande quantidade de nomes de domínio periodicamente que podem ser usados como pontos de encontro com seus servidores de comando e controle (C&C). Os servidores de comando e controle são computadores que emitem comandos para membros de um botnet, ou seja, uma coleção de dispositivos conectados à Internet infectados e controlados por um tipo comum de malware. O grande número de pontos de encontro potenciais dificulta o encerramento efetivo dos botnets, uma vez que os computadores infectados tentam entrar em contato com alguns desses nomes de domínio todos os dias para receber atualizações ou comandos.

> **Note**
>
> Essa descoberta é baseada na análise de nomes de domínio usando heurística avançada e pode identificar novos domínios de DGA que não estão presentes em feeds de inteligência contra ameaças.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Trojan:EC2/DGADomainRequest.C!DNS

Uma instância do EC2 está consultando domínios gerados por algoritmos. Esses domínios são comumente usados por malware e podem ser um indicativo de uma instância do EC2 comprometida.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância do EC2 listada no seu ambiente da AWS está tentando consultar domínios do algoritmo de geração de domínio (DGA). Sua instância do EC2 pode estar comprometida.

Os DGAs são usados para gerar uma grande quantidade de nomes de domínio periodicamente que podem ser usados como pontos de encontro com seus servidores de comando e controle (C&C). Os servidores de comando e controle são computadores que emitem comandos para membros de um botnet, ou seja, uma coleção de dispositivos conectados à Internet infectados e controlados por um tipo comum de malware. O grande número de pontos de encontro potenciais dificulta o encerramento efetivo dos botnets, uma vez que os computadores infectados tentam entrar em contato com alguns desses nomes de domínio todos os dias para receber atualizações ou comandos.

> **Note**
>
> Essa descoberta é baseada em domínios DGA conhecidos dos feeds de inteligência de ameaças GuardDuty da.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Trojan:EC2/DNSDataExfiltration

Uma instância do EC2 está exfiltrando dados por meio de consultas DNS.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa que a instância do EC2 listada em seu ambiente da AWS está executando um malware que usa consultas ao DNS para transferências de dados de saída. Esse tipo de transferência de dados é indicativo de uma instância comprometida e pode resultar na exfiltração de dados. Normalmente, o tráfego de DNS não é bloqueado por firewalls. Por exemplo, o malware em uma instância do EC2 comprometida pode codificar dados (ex.: seu número de cartão de crédito) em uma consulta DNS e enviá-los para um servidor DNS remoto controlado por um invasor.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Trojan:EC2/DriveBySourceTraffic!DNS

Uma instância do EC2 está consultando um nome de domínio de um host remoto que é uma fonte conhecida de ataques Drive-by download.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa a você que uma instância do EC2 em seu ambiente da AWS pode estar comprometida porque está consultando um nome de domínio de um host remoto que é uma fonte conhecida de ataques Drive-by download. Estes são downloads indesejados de software de computador da Internet que podem acionar uma instalação automática de vírus, spyware ou malware.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Trojan:EC2/DropPoint

Uma instância do EC2 está tentando se comunicar com um endereço IP de um host remoto que é conhecido por manter credenciais e outros dados roubados capturados por malware.

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que uma instância do EC2 em seu ambiente da AWS está tentando se comunicar com um endereço IP de um host remoto que é conhecido por manter credenciais e outros dados roubados capturados por malware.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Trojan:EC2/DropPoint!DNS

Uma instância do EC2 está consultando um nome de domínio de um host remoto que é conhecido por manter credenciais e outros dados roubados capturados por malware.

Gravidade padrão: média

- Fonte de dados: logs de DNS

Essa descoberta informa a você que uma instância do EC2 em seu ambiente da AWS está consultando um nome de domínio de um host remoto que é conhecido por manter credenciais e outros dados roubados capturados por malware.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Trojan:EC2/PhishingDomainRequest!DNS

Uma instância do EC2 está consultando domínios envolvidos em ataques de phishing. Sua instância do EC2 pode estar comprometida.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa que existe uma instância do EC2 no seu ambiente da AWS que está tentando consultar um domínio envolvido em ataques de phishing. Domínios de phishing são configuradas por alguém se passando por uma instituição legítima para induzir indivíduos a fornecerem dados confidenciais, como informações de identificação pessoal, dados bancários e de cartão de crédito, e senhas. Sua instância do EC2 pode estar tentando recuperar dados confidenciais armazenados em um site de phishing ou configurar um site de phishing. Sua instância do EC2 pode estar comprometida.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom

Uma instância do EC2 está fazendo conexões com um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: média

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que uma instância do EC2 em seu ambiente da AWS está se comunicando com um endereço IP incluído em uma lista de ameaças que você carregou. Em GuardDuty, uma lista de ameaças consiste em endereços IP maliciosos conhecidos. GuardDuty gera descobertas com base em listas de ameaças enviadas. A lista de ameaças usada para gerar essa descoberta será listada nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

UnauthorizedAccess:EC2/MetadataDNSRebind

Uma instância do EC2 está executando pesquisas de DNS que são resolvidas como o serviço de metadados da instância.

Gravidade padrão: alta

- Fonte de dados: logs de DNS

Essa descoberta informa que uma instância do EC2 no seu ambiente da AWS está consultando um domínio que é resolvido como o endereço IP dos metadados do EC2 (169.254.169.254). Uma consulta ao DNS desse tipo pode indicar que a instância é alvo de uma técnica de revinculação de DNS. Essa técnica pode ser usada para obter metadados de uma instância do EC2, incluindo as credenciais do IAM associadas à instância.

A revinculação de DNS envolve enganar um aplicativo em execução na instância do EC2 para carregar dados de retorno de um URL, onde o nome de domínio no URL é resolvido como o endereço IP de metadados do EC2 (169.254.169.254). Isso faz com que o aplicativo acesse metadados do EC2 e possivelmente os disponibilize para o invasor.

É possível acessar metadados do EC2 usando a revinculação de DNS somente se a instância do EC2 estiver executando um aplicativo vulnerável que permita a injeção de URLs ou se um usuário humano acessar a URL em um navegador da web em execução na instância do EC2.

Recomendações de correção:

Em resposta a essa descoberta, você deve avaliar se há um aplicativo vulnerável em execução na instância do EC2 ou se um usuário humano usou um navegador para acessar o domínio identificado na descoberta. Se a causa raiz for um aplicativo vulnerável, você deverá corrigir a vulnerabilidade. Se alguém navegou pelo domínio identificado, você deve bloquear o domínio ou evitar que os usuários o acessem. Se você determinar que essa descoberta estava relacionada a qualquer um dos casos acima, deverá revogar a sessão associada à instância do EC2.

Alguns clientes da AWS mapeiam intencionalmente o endereço IP dos metadados para um nome de domínio em seus servidores DNS autoritativas. Se esse for o caso em seu ambiente da ,

recomendamos configurar uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `UnauthorizedAccess:EC2/MetaDataDNSRebind`. O segundo critério de filtro deve ser o domínio de solicitação de DNS e o valor deve corresponder ao domínio mapeado para o endereço IP de metadados (169.254.169.254). Para obter mais informações sobre como criar regras de supressão, consulte Regras de supressão.

UnauthorizedAccess:EC2/RDPBruteForce

Uma instância do EC2 esteve envolvida em ataques de força bruta do RDP.

Gravidade padrão: baixa*

> **Note**
>
> A gravidade dessa descoberta é baixa se a instância do EC2 foi o alvo de um ataque de força bruta. A gravidade dessa descoberta será alta se sua instância do EC2 for o agente que está sendo usado para executar o ataque de força bruta.

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que uma instância do EC2 no seu ambiente da AWS esteve envolvida em um ataque de força bruta destinado a obter senhas para serviços de RDP em sistemas baseados no Windows. Isso pode indicar acesso não autorizado aos seus recursos da AWS.

Recomendações de correção:

Se a Função do recurso da instância é `ACTOR`, isso indica que a instância foi usada para executar ataques de força bruta RDP. A menos que essa instância tenha um motivo legítimo para entrar em contato com o endereço IP listado como o `Target`, é recomendável que você presuma que a instância foi comprometida e execute as ações listadas em Correção de uma instância potencialmente comprometida do Amazon EC2.

Se a Função do recurso da instância é `TARGET`, essa descoberta pode ser corrigida protegendo a porta RDP somente para IPs confiáveis por meio de grupos de segurança, ACLs ou firewalls. Para obter mais informações, consulte Dicas para proteger suas instâncias do EC2 (Linux).

UnauthorizedAccess:EC2/SSHBruteForce

Uma instância do EC2 esteve envolvida em ataques de força bruta do SSH.

Gravidade padrão: baixa*

> **Note**
>
> A gravidade dessa descoberta será baixa se um ataque de força bruta for destinado a uma de suas instâncias do EC2. A gravidade dessa descoberta será alta se sua instância do EC2 estiver sendo usada para executar o ataque de força bruta.

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que uma instância do EC2 no seu ambiente da AWS estava envolvida em um ataque de força bruta destinado a obter senhas para serviços de SSH em sistemas baseados no Linux. Isso pode indicar acesso não autorizado aos seus recursos da AWS.

> **Note**
>
> Essa descoberta é gerada apenas por meio do monitoramento de tráfego do na porta 22. Se os serviços SSH estiverem configurados para usar outras portas, essa descoberta não será gerada.

Recomendações de correção:

Se o alvo da tentativa de força bruta for um bastion host, isso pode representar um comportamento esperado para o ambiente da AWS. Se for esse o caso, recomendamos configurar uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `UnauthorizedAccess:EC2/SSHBruteForce`. O segundo critério de filtro deve corresponder à instância ou às instâncias que servem como um bastion host. É possível usar o atributo ID da imagem da instância ou o atributo de valor da Tag dependendo de quais critérios forem identificáveis

com as instâncias que hospedam essas ferramentas. Para obter mais informações sobre como criar regras de supressão, consulte Regras de supressão.

Se essa atividade não for esperada para o ambiente e a Função do recurso da instância for `TARGET`, essa descoberta poderá ser corrigida protegendo a porta SSH somente para IPs confiáveis por meio de grupos de segurança, ACLs ou firewalls. Para obter mais informações, consulte Dicas para proteger sua instância do EC2.

Se a Função do recurso da instância for `ACTOR` isso indicará que a instância foi usada para executar ataques de força bruta do SSH. A menos que essa instância tenha um motivo legítimo para entrar em contato com o endereço IP listado como o `Target`, é recomendável que você presuma que a instância foi comprometida e execute as ações listadas em Correção de uma instância potencialmente comprometida do Amazon EC2.

UnauthorizedAccess:EC2/TorClient

A instância do EC2 está fazendo conexões com um Tor Guard ou um nó de autoridade.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que uma instância do EC2 em seu ambiente da AWS está fazendo conexões com um Tor Guard ou um nó de autoridade. Tor é um software para permitir a comunicação anônima. Tor Guards ou nós de autoridade atuam como gateways iniciais em uma rede do Tor. Esse tráfego pode indicar que a instância do EC2 foi comprometida está atuando como um cliente em uma rede do Tor. Essa descoberta pode indicar acesso não autorizado aos seus recursos da AWS com a intenção de ocultar a verdadeira identidade do invasor.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

UnauthorizedAccess:EC2/TorRelay

A instância do EC2 está fazendo conexões com uma rede do Tor como uma retransmissão Tor.

Gravidade padrão: alta

- Fonte de dados: logs de fluxo da VPC

Essa descoberta informa que uma instância do EC2 em seu ambiente da AWS está fazendo conexões com uma rede do Tor de uma maneira que sugere que ela esteja atuando como uma retransmissão Tor. Tor é um software para permitir a comunicação anônima. Retransmissões Tor aumentam o anonimato da comunicação encaminhando o tráfego possivelmente ilícito do cliente de uma retransmissão Tor para outra.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para ter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

GuardDuty Tipos de descoberta do IAM

As descobertas a seguir são específicas de entidades e chaves de acesso do IAM e sempre têm um Tipo de recurso igual a `AccessKey`. A gravidade e os detalhes das descobertas serão diferentes com base no tipo de descoberta.

As descobertas listadas aqui incluem as fontes de dados e os modelos usados para gerar esse tipo de descoberta. Para ter mais informações, consulte Fontes de dados fundamentais.

Para todas as descobertas relacionadas ao IAM, recomendamos que você examine a entidade em questão e garanta que suas permissões sigam a melhor prática de privilégio mínimo. Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Consulte . Para obter mais informações sobre correção de descobertas, consulte Correção de credenciais potencialmente comprometidas AWS.

Tópicos

- CredentialAccess:IAMUser/AnomalousBehavior
- DefenseEvasion:IAMUser/AnomalousBehavior
- Discovery:IAMUser/AnomalousBehavior
- Exfiltration:IAMUser/AnomalousBehavior
- Impact:IAMUser/AnomalousBehavior

- InitialAccess:IAMUser/AnomalousBehavior
- PenTest:IAMUser/KaliLinux
- PenTest:IAMUser/ParrotLinux
- PenTest:IAMUser/PentooLinux
- Persistence:IAMUser/AnomalousBehavior
- Policy:IAMUser/RootCredentialUsage
- PrivilegeEscalation:IAMUser/AnomalousBehavior
- Recon:IAMUser/MaliciousIPCaller
- Recon:IAMUser/MaliciousIPCaller.Custom
- Recon:IAMUser/TorIPCaller
- Stealth:IAMUser/CloudTrailLoggingDisabled
- Stealth:IAMUser/PasswordPolicyChange
- UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
- UnauthorizedAccess:IAMUser/MaliciousIPCaller
- UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom
- UnauthorizedAccess:IAMUser/TorIPCaller

CredentialAccess:IAMUser/AnomalousBehavior

Uma API usada para obter acesso a um AWS ambiente foi invocada de forma anômala.

Gravidade padrão: média

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma solicitação de API anômala foi observada em sua conta. Essa descoberta pode incluir uma única API ou uma série de solicitações de API relacionadas feitas nas proximidades por uma única identidade de usuário. Comumente, a API observada é associada ao estágio de acesso às credenciais de um ataque quando um adversário está tentando coletar

senhas, nomes de usuário e chaves de acesso para seu ambiente. As APIs nesta categoria são `GetPasswordData`, `GetSecretValue` e `GenerateDbAuthToken`.

Essa solicitação de API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo de ML rastreia vários fatores da solicitação de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e a API específica que foi solicitada. Os detalhes sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação podem ser encontrados nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

DefenseEvasion:IAMUser/AnomalousBehavior

Uma API usada para evitar medidas defensivas foi invocada de forma anômala.

Gravidade padrão: média

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma solicitação de API anômala foi observada em sua conta. Essa descoberta pode incluir uma única API ou uma série de solicitações de API relacionadas feitas nas proximidades por uma única identidade de usuário. Comumente, a API observada é associada a táticas de evasão de defesa, nas quais um adversário está tentando encobrir seus rastros e evitar ser detectado. As APIs nessa categoria geralmente são operações de exclusão, desabilitação ou interrupção, como `DeleteFlowLogs`, `DisableAlarmActions` ou `StopLogging`.

Essa solicitação de API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo de ML rastreia vários fatores da solicitação de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e a API específica que foi solicitada. Os detalhes sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação podem ser encontrados nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

Discovery:IAMUser/AnomalousBehavior

Uma API comumente usada para descobrir recursos foi invocada de forma anômala.

Gravidade padrão: baixa

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma solicitação de API anômala foi observada em sua conta. Essa descoberta pode incluir uma única API ou uma série de solicitações de API relacionadas feitas nas proximidades por uma única identidade de usuário. A API observada é comumente associada ao estágio de descoberta de um ataque, quando um adversário coleta informações para determinar se seu AWS ambiente é suscetível a um ataque mais amplo. As APIs nessa categoria geralmente são operações de obtenção, descrição ou lista, como `DescribeInstances`, `GetRolePolicy` ou `ListAccessKeys`.

Essa solicitação de API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo de ML rastreia vários fatores da solicitação de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e a API específica que foi solicitada. Os detalhes sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação podem ser encontrados nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

Exfiltration:IAMUser/AnomalousBehavior

Uma API comumente usada para coletar dados de um AWS ambiente foi invocada de forma anômala.

Gravidade padrão: alta

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma solicitação de API anômala foi observada em sua conta. Essa descoberta pode incluir uma única API ou uma série de solicitações de API relacionadas feitas nas proximidades por uma única identidade de usuário. Comumente, a API observada é associada a táticas de exfiltração em que um adversário está tentando coletar dados de sua rede usando empacotamento e criptografia para evitar a detecção. As APIs para esse tipo de descoberta são apenas operações de gerenciamento (ambiente de gerenciamento) e geralmente estão relacionadas ao S3, aos snapshots e aos bancos de dados, como `PutBucketReplication`, `CreateSnapshot` ou `RestoreDBInstanceFromDBSnapshot`.

Essa solicitação de API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo de ML rastreia vários fatores da solicitação de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e a API específica que foi solicitada. Os detalhes sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação podem ser encontrados nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

Impact:IAMUser/AnomalousBehavior

Uma API comumente usada para adulterar dados ou processos em um AWS ambiente foi invocada de forma anômala.

Gravidade padrão: alta

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma solicitação de API anômala foi observada em sua conta. Essa descoberta pode incluir uma única API ou uma série de solicitações de API relacionadas feitas nas

proximidades por uma única identidade de usuário. Comumente, a API observada é associada a táticas de impacto em que um adversário está tentando interromper as operações e manipular, interromper ou destruir dados em sua conta. As APIs para esse tipo de descoberta geralmente são operações de exclusão, atualização ou colocação, como `DeleteSecurityGroup`, `UpdateUser` ou `PutBucketPolicy`.

Essa solicitação de API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo de ML rastreia vários fatores da solicitação de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e a API específica que foi solicitada. Os detalhes sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação podem ser encontrados nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

InitialAccess:IAMUser/AnomalousBehavior

Uma API comumente usada para obter acesso não autorizado a um AWS ambiente foi invocada de forma anômala.

Gravidade padrão: média

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma solicitação de API anômala foi observada em sua conta. Essa descoberta pode incluir uma única API ou uma série de solicitações de API relacionadas feitas nas proximidades por uma única identidade de usuário. Comumente, a API observada é associada ao estágio inicial de acesso de um ataque, quando um adversário está tentando estabelecer acesso ao seu ambiente. As APIs nessa categoria geralmente são operações de token de obtenção ou de sessão, como `GetFederationToken`, `StartSession` ou `GetAuthorizationToken`.

Essa solicitação de API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo

de ML rastreia vários fatores da solicitação de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e a API específica que foi solicitada. Os detalhes sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação podem ser encontrados nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

PenTest:IAMUser/KaliLinux

Uma API foi invocada de uma máquina Linux Kali.

Gravidade padrão: média

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma máquina executando o Kali Linux está fazendo chamadas de API usando credenciais que pertencem à AWS conta listada em seu ambiente. O Kali Linux é uma ferramenta popular de teste de penetração que profissionais de segurança usam para identificar vulnerabilidades nas instâncias do EC2 que exigem correções. Os invasores também usam essa ferramenta para encontrar pontos fracos na configuração do EC2 e obter acesso não autorizado ao seu ambiente. AWS

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

PenTest:IAMUser/ParrotLinux

Uma API foi invocada a partir de uma máquina Parrot Security Linux.

Gravidade padrão: média

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma máquina executando o Parrot Security Linux está fazendo chamadas de API usando credenciais que pertencem à AWS conta listada em seu ambiente. O Parrot Security Linux é uma ferramenta popular de teste de penetração que profissionais de segurança usam para identificar vulnerabilidades nas instâncias do EC2 que exigem correções. Os invasores também usam essa ferramenta para encontrar pontos fracos na configuração do EC2 e obter acesso não autorizado ao seu ambiente. AWS

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

PenTest:IAMUser/PentooLinux

Uma API foi invocada a partir de uma máquina Pentoo Linux.

Gravidade padrão: média

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma máquina executando o Pentoo Linux está fazendo chamadas de API usando credenciais que pertencem à AWS conta listada em seu ambiente. O Pentoo Linux é uma ferramenta popular de teste de penetração que profissionais de segurança usam para identificar vulnerabilidades nas instâncias do EC2 que exigem correções. Os invasores também usam essa ferramenta para encontrar pontos fracos na configuração do EC2 e obter acesso não autorizado ao seu ambiente. AWS

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

Persistence:IAMUser/AnomalousBehavior

Uma API comumente usada para manter o acesso não autorizado a um AWS ambiente foi invocada de forma anômala.

Gravidade padrão: média

- Fonte de dados: evento CloudTrail de gerenciamento

Essa descoberta informa que uma solicitação de API anômala foi observada em sua conta. Essa descoberta pode incluir uma única API ou uma série de solicitações de API relacionadas feitas nas proximidades por uma única identidade de usuário. Comumente, a API observada é associada a táticas de persistência em que um adversário obteve acesso ao seu ambiente e está tentando manter esse acesso. As APIs nessa categoria geralmente são operações de criação, importação ou modificação, como `CreateAccessKey`, `ImportKeyPair` ou `ModifyInstanceAttribute`.

Essa solicitação de API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo de ML rastreia vários fatores da solicitação de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e a API específica que foi solicitada. Os detalhes sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação podem ser encontrados nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

Policy:IAMUser/RootCredentialUsage

Foi invocada uma API usando credenciais de login do usuário raiz.

Gravidade padrão: baixa

- Fonte de dados: eventos CloudTrail de gerenciamento ou eventos CloudTrail de dados

Essa descoberta informa que as credenciais de login do usuário raiz da Conta da AWS listada em seu ambiente estão sendo usadas para fazer solicitações aos serviços da AWS . É recomendável que os usuários nunca usem as credenciais de login do usuário root para acessar os serviços. AWS Em vez disso, AWS os serviços devem ser acessados usando credenciais temporárias de privilégio mínimo de AWS Security Token Service (STS). Para situações em que o AWS STS não é compatível, é recomendável usar credenciais de usuário do IAM. Para obter mais informações, consulte Melhores práticas do IAM.

> **Note**
>
> Se a detecção de ameaças do S3 estiver habilitada para a conta, essa descoberta poderá ser gerada em resposta às tentativas de executar operações do plano de dados do S3 nos recursos do S3 usando as credenciais de login do usuário raiz da Conta da AWS. A chamada de API usada será listada nos detalhes da descoberta. Se a detecção de ameaças do S3 não estiver habilitada, essa descoberta só poderá ser acionada pelas APIs de registro de eventos. Para obter mais informações sobre a detecção de ameaças do S3, consulte Proteção do S3.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

PrivilegeEscalation:IAMUser/AnomalousBehavior

Uma API comumente usada para obter permissões de alto nível para um AWS ambiente foi invocada de forma anômala.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que uma solicitação de API anômala foi observada em sua conta. Essa descoberta pode incluir uma única API ou uma série de solicitações de API relacionadas feitas nas proximidades por uma única identidade de usuário. Comumente, a API observada é associada a táticas de escalonamento de privilégios em que um adversário está tentando obter permissões de nível superior para um ambiente. As APIs nessa categoria geralmente envolvem operações que alteram políticas, perfis e usuários do IAM, como `AssociateIamInstanceProfile`, `AddUserToGroup` ou `PutUserPolicy`.

Essa solicitação de API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo de ML rastreia vários fatores da solicitação de API, como o usuário que fez a solicitação, o local de

onde a solicitação foi feita e a API específica que foi solicitada. Os detalhes sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação podem ser encontrados nos detalhes da descoberta.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

Recon:IAMUser/MaliciousIPCaller

Uma API foi invocada a partir de um endereço IP mal-intencionado conhecido.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que uma operação de API que pode listar ou descrever recursos em uma conta no seu ambiente da AWS foi invocada a partir de um endereço IP incluído em uma lista de ameaças. Um invasor pode usar credenciais roubadas para realizar esse tipo de reconhecimento de seus AWS recursos a fim de encontrar credenciais mais valiosas ou determinar as capacidades das credenciais que ele já possui.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

Recon:IAMUser/MaliciousIPCaller.Custom

Uma API foi invocada a partir de um endereço IP mal-intencionado conhecido.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que uma operação de API que pode listar ou descrever recursos em uma conta dentro do seu ambiente da AWS foi invocada a partir de um endereço IP incluído em uma lista de ameaças personalizada. A lista de ameaças usada será listada nos detalhes da descoberta. Um

invasor pode usar credenciais roubadas para realizar esse tipo de reconhecimento de seus AWS recursos a fim de encontrar credenciais mais valiosas ou determinar as capacidades das credenciais que ele já possui.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

Recon:IAMUser/TorIPCaller

Uma API foi invocada a partir de um endereço IP do nó de saída do Tor.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que uma operação de API que pode listar ou descrever recursos em uma conta no seu ambiente da AWS foi invocada de um endereço IP de nó de saída Tor. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Um atacante usaria o Tor para mascarar sua verdadeira identidade.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

Stealth:IAMUser/CloudTrailLoggingDisabled

AWS CloudTrail o registro foi desativado.

Gravidade padrão: baixa

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que uma CloudTrail trilha em seu AWS ambiente foi desativada. Isso pode ser uma tentativa de um invasor de desabilitar a gravação de logs para não deixar rastros, eliminando quaisquer evidências da atividade dele ao obter acesso aos seus recursos da AWS

para fins mal-intencionados. Essa descoberta pode ser acionada por uma exclusão bem-sucedida ou atualização de uma trilha. Essa descoberta também pode ser acionada por uma exclusão bem-sucedida de um bucket do S3 que armazena os registros de uma trilha associada a. GuardDuty

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

Stealth:IAMUser/PasswordPolicyChange

A política de senha da conta foi enfraquecida.

Gravidade padrão: baixa*

> **Note**
>
> A gravidade dessa descoberta pode ser baixa, média ou alta, dependendo da gravidade das alterações feitas na política de senhas.

- Fonte de dados: eventos CloudTrail de gerenciamento

A política de senha da AWS conta foi enfraquecida na conta listada em seu AWS ambiente. Por exemplo, ela foi excluída ou atualizada para exigir menos caracteres, não requer símbolos nem números, ou obrigada a prolongar o período de validade da senha. Essa descoberta também pode ser desencadeada por uma tentativa de atualizar ou excluir a política de senha AWS da sua conta. A política de senha da AWS conta define as regras que regem quais tipos de senhas podem ser definidos para seus usuários do IAM. Uma política de senha mais fraca permite a criação de senhas fáceis de lembrar e possivelmente mais fáceis de adivinhar, criando um risco à segurança.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B

Foram observados vários logins de console bem-sucedidos em todo o mundo.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que foram observados vários logins bem-sucedidos no console para o mesmo usuário do IAM, ao mesmo tempo e em vários locais geográficos diferentes. Esses padrões de localização de acesso anômalos e arriscados indicam um possível acesso não autorizado aos seus recursos. AWS

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS

As credenciais criadas exclusivamente para uma instância do EC2 pela função de execução de uma instância estão sendo usadas de outra conta na AWS.

Gravidade padrão: alta*

> **Note**
>
> A gravidade padrão desta descoberta é baixa. No entanto, se a API foi invocada por uma conta afiliada ao seu AWS ambiente, a gravidade é Média.

- Fonte de dados: eventos CloudTrail de gerenciamento ou eventos de dados do S3

Essa descoberta informa quando suas credenciais de instância do EC2 são usadas para invocar APIs de um endereço IP que pertence a uma AWS conta diferente daquela em que a instância EC2 associada está sendo executada.

AWS não recomenda redistribuir credenciais temporárias fora da entidade que as criou (por exemplo, AWS aplicativos, EC2 ou Lambda). No entanto, os usuários autorizados podem exportar

credenciais das suas respectivas instâncias do EC2 para fazer chamadas de API legítimas. Se o `remoteAccountDetails.Affiliated` campo for, `True` a API foi invocada de uma conta associada ao seu AWS ambiente. Para descartar um possível ataque e verificar a legitimidade da atividade, entre em contato com o usuário do IAM para quem essas credenciais estão atribuídas.

> **Note**
>
> Se GuardDuty observar a atividade contínua de uma conta remota, seu modelo de aprendizado de máquina (ML) identificará isso como um comportamento esperado. Portanto, GuardDuty deixará de gerar essa descoberta para atividades dessa conta remota. GuardDuty continuará gerando descobertas sobre novos comportamentos de outras contas remotas e reavaliará as contas remotas aprendidas à medida que o comportamento muda com o tempo.

Recomendações de correção:

Em resposta a essa descoberta, é possível usar o seguinte fluxo de trabalho para determinar um curso de ação:

1. Identifique a conta remota envolvida no campo `service.action.awsApiCallAction.remoteAccountDetails.accountId`.
2. Em seguida, determine se essa conta está afiliada ao seu GuardDuty ambiente a partir do `service.action.awsApiCallAction.remoteAccountDetails.affiliated` campo.
3. Se a conta for afiliada, entre em contato com o proprietário da conta remota e com o proprietário das credenciais da instância EC2 para investigar.
4. Se a conta não for afiliada, primeiro avalie se a conta está associada à sua organização, mas não faz parte da configuração de GuardDuty várias contas ou se ainda não GuardDuty foi ativada na conta. Caso contrário, entre em contato com o proprietário das credenciais do EC2 para determinar se há um caso de uso para uma conta remota usar essas credenciais.
5. Se o proprietário das credenciais não reconhecer a conta remota, as credenciais podem ter sido comprometidas por um agente de ameaça operando na AWS. Siga as etapas recomendadas em Correção de uma instância potencialmente comprometida do Amazon EC2 para proteger seu ambiente. Além disso, você pode enviar uma denúncia de abuso à equipe de AWS Confiança e Segurança para iniciar uma investigação sobre a conta remota. Ao enviar seu relatório para o AWS Trust and Safety, inclua todos os detalhes do JSON da descoberta.

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS

As credenciais criadas exclusivamente para uma instância do EC2 pela função de execução de uma instância estão sendo usadas por um endereço IP externo.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de gerenciamento ou eventos de dados do S3

Essa descoberta informa que um host externo AWS tentou executar operações de AWS API usando AWS credenciais temporárias que foram criadas em uma instância do EC2 em seu ambiente. AWS A instância EC2 listada pode estar comprometida e as credenciais temporárias dessa instância podem ter sido transferidas para um host remoto externo. AWS AWS não recomenda redistribuir credenciais temporárias fora da entidade que as criou (por exemplo, AWS aplicativos, EC2 ou Lambda). No entanto, os usuários autorizados podem exportar credenciais das suas respectivas instâncias do EC2 para fazer chamadas de API legítimas. Para descartar um possível ataque e verificar a legitimidade da atividade, valide se o uso de credenciais de instância do IP remoto na descoberta é esperado.

> **Note**
>
> Se GuardDuty observar a atividade contínua de uma conta remota, seu modelo de aprendizado de máquina (ML) identificará isso como um comportamento esperado. Portanto, GuardDuty deixará de gerar essa descoberta para atividades dessa conta remota. GuardDuty continuará gerando descobertas sobre novos comportamentos de outras contas remotas e reavaliará as contas remotas aprendidas à medida que o comportamento muda com o tempo.

Recomendações de correção:

Essa descoberta é gerada quando a rede é configurada para rotear o tráfego da Internet de modo que ele saia de um gateway on-premises e não de um gateway da Internet (IGW) da VPC. Configurações comuns, como usar AWS Outposts, ou conexões de VPN da VPC podem resultar em tráfego roteado dessa maneira. Se esse comportamento for esperado, é recomendável usar regras de supressão e criar uma regra que consista em dois critérios de filtro. O primeiro critério é tipo de descoberta, que deve ser `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. O segundo critério de filtro é o endereço

IPv4 do chamador de API com o endereço IP ou intervalo CIDR do seu gateway da Internet on-premises. Para saber mais sobre a criação de regras de supressão, consulte Regras de supressão.

> **Note**
>
> Se GuardDuty observar a atividade contínua de uma fonte externa, seu modelo de aprendizado de máquina identificará isso como comportamento esperado e deixará de gerar essa descoberta para atividades dessa fonte. GuardDuty continuará gerando descobertas sobre novos comportamentos a partir de outras fontes e reavaliará as fontes aprendidas à medida que o comportamento muda com o tempo.

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Consulte Correção de credenciais potencialmente comprometidas AWS.

UnauthorizedAccess:IAMUser/MaliciousIPCaller

Uma API foi invocada a partir de um endereço IP mal-intencionado conhecido.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que uma operação de API (por exemplo, uma tentativa de iniciar uma instância do EC2, criar um novo usuário do IAM ou modificar seus AWS privilégios) foi invocada a partir de um endereço IP malicioso conhecido. Isso pode indicar acesso não autorizado aos AWS recursos em seu ambiente.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom

Uma API foi invocada a partir de um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que uma operação de API (por exemplo, uma tentativa de iniciar uma instância do EC2, criar um novo usuário do IAM ou modificar AWS privilégios) foi invocada a partir de um endereço IP incluído em uma lista de ameaças que você enviou. No , uma lista de ameaças consiste em endereços IP mal-intencionados conhecidos. Isso pode indicar acesso não autorizado aos AWS recursos em seu ambiente.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

UnauthorizedAccess:IAMUser/TorIPCaller

Uma API foi invocada a partir de um endereço IP do nó de saída do Tor.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que uma operação da API (por exemplo, uma tentativa de iniciar uma instância do EC2, criar um novo usuário do IAM ou modificar seus privilégios da AWS) foi invocada a partir de um endereço IP de nó de saída do Tor. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar um acesso não autorizado aos seus recursos da AWS com a intenção de ocultar a verdadeira identidade do invasor.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

Tipos de descobertas de logs de auditoria do Kubernetes

As descobertas a seguir são específicas para os recursos do Kubernetes e terão um resource_type de `EKSCluster`. A gravidade e os detalhes das descobertas serão diferentes com base no tipo de descoberta.

Para todas as descobertas do tipo Kubernetes, recomendamos que você examine o recurso em questão para determinar se a atividade é esperada ou potencialmente mal-intencionada. Para obter orientação sobre como remediar um recurso comprometido do Kubernetes identificado por uma descoberta, consulte. GuardDuty Como corrigir os resultados do Monitoramento de logs de auditoria do EKS

> **Note**
>
> Se a atividade pela qual essas descobertas são geradas for esperada, considere adicionar Regras de supressão para evitar futuros alertas.

Tópicos

- CredentialAccess:Kubernetes/MaliciousIPCaller
- CredentialAccess:Kubernetes/MaliciousIPCaller.Custom
- CredentialAccess:Kubernetes/SuccessfulAnonymousAccess
- CredentialAccess:Kubernetes/TorIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller
- DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom
- DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess
- DefenseEvasion:Kubernetes/TorIPCaller
- Discovery:Kubernetes/MaliciousIPCaller
- Discovery:Kubernetes/MaliciousIPCaller.Custom
- Discovery:Kubernetes/SuccessfulAnonymousAccess
- Discovery:Kubernetes/TorIPCaller
- Execution:Kubernetes/ExecInKubeSystemPod
- Impact:Kubernetes/MaliciousIPCaller
- Impact:Kubernetes/MaliciousIPCaller.Custom
- Impact:Kubernetes/SuccessfulAnonymousAccess
- Impact:Kubernetes/TorIPCaller
- Persistence:Kubernetes/ContainerWithSensitiveMount
- Persistence:Kubernetes/MaliciousIPCaller
- Persistence:Kubernetes/MaliciousIPCaller.Custom

- Persistence:Kubernetes/SuccessfulAnonymousAccess
- Persistence:Kubernetes/TorIPCaller
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/KubeflowDashboardExposed
- PrivilegeEscalation:Kubernetes/PrivilegedContainer
- CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated
- Execution:Kubernetes/AnomalousBehavior.ExecInPod
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer
- Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount
- Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed
- PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated
- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

> **Note**
>
> Antes da versão 1.14 do Kubernetes, o `system:unauthenticated` grupo era associado e por padrão. `system:discovery` `system:basic-user` ClusterRoles Essa associação pode permitir o acesso não intencional de usuários anônimos. As atualizações do cluster não revogam essas permissões. Mesmo que você tenha atualizado seu cluster para a versão 1.14 ou superior, essas permissões ainda poderão estar habilitadas. Recomendamos que você desassocie essas permissões do grupo `system:unauthenticated`. Para obter orientação sobre a revogação dessas permissões, consulte as melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS.

CredentialAccess:Kubernetes/MaliciousIPCaller

Uma API comumente usada para acessar credenciais ou segredos em um cluster do Kubernetes foi invocada a partir de um endereço IP mal-intencionado conhecido.

Gravidade padrão: alta

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação de API foi invocada a partir de um endereço IP associado a atividades mal-intencionadas conhecidas. Comumente, a API observada é associada às táticas de acesso a credenciais em que um adversário está tentando coletar senhas, nomes de usuário e chaves de acesso para seu cluster do Kubernetes.

Recomendações de correção:

Se o usuário relatado na descoberta abaixo da `KubernetesUserDetails` seção `ésystem:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogar as permissões, se necessário, seguindo as instruções nas melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

CredentialAccess:Kubernetes/MaliciousIPCaller.Custom

Uma API comumente usada para acessar credenciais ou segredos em um cluster do Kubernetes foi invocada a partir de um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: alta

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação de API foi invocada a partir de um endereço IP incluído em uma lista de ameaças que você carregou. A lista de ameaças associada a essa descoberta está listada na seção Informações adicionais dos detalhes de uma descoberta. Comumente, a API observada é associada às táticas de acesso a credenciais em que um adversário está tentando coletar senhas, nomes de usuário e chaves de acesso para seu cluster do Kubernetes.

Recomendações de correção:

Se o usuário relatado na descoberta abaixo da `KubernetesUserDetails` seção é`system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogar as permissões, se necessário, seguindo as instruções nas melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

CredentialAccess:Kubernetes/SuccessfulAnonymousAccess

Uma API comumente usada para acessar credenciais ou segredos em um cluster do Kubernetes foi invocada por um usuário não autenticado.

Gravidade padrão: alta

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação de API foi invocada com sucesso pelo usuário `system:anonymous`. As chamadas de API feitas por `system:anonymous` não são autenticadas. Comumente, a API observada é associada às táticas de acesso a credenciais em que um adversário está tentando coletar senhas, nomes de usuário e chaves de acesso para seu cluster do Kubernetes. Essa atividade indica que o acesso anônimo ou não autenticado é permitido na ação da API relatada na descoberta e pode ser permitido em outras ações. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais estão comprometidas.

Recomendações de correção:

Você deve examinar as permissões que foram concedidas ao usuário `system:anonymous` em seu cluster e garantir que todas as permissões sejam necessárias. Se as permissões foram concedidas por engano ou de maneira mal-intencionada, você deve revogar o acesso do usuário e reverter as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS.

Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

CredentialAccess:Kubernetes/TorIPCaller

Uma API comumente usada para acessar credenciais ou segredos em um cluster do Kubernetes foi invocada a partir de um endereço IP do nó de saída do Tor.

Gravidade padrão: alta

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação da API foi invocada a partir de um endereço IP do nó de saída do Tor. Comumente, a API observada é associada às táticas de acesso a credenciais em que um adversário está tentando coletar senhas, nomes de usuário e chaves de acesso para seu cluster do Kubernetes. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar acesso não autorizado aos recursos do cluster do Kubernetes com a intenção de ocultar a verdadeira identidade do invasor.

Recomendações de correção:

Se o usuário relatado na descoberta abaixo da `KubernetesUserDetails` seção `ésystem:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogar as permissões, se necessário, seguindo as instruções nas melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

DefenseEvasion:Kubernetes/MaliciousIPCaller

Uma API comumente usada para evitar medidas defensivas foi invocada a partir de um endereço IP mal-intencionado conhecido.

Gravidade padrão: alta

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação de API foi invocada a partir de um endereço IP associado a atividades mal-intencionadas conhecidas. Comumente, a API observada é associada a táticas de evasão de defesa, nas quais um adversário está tentando esconder suas ações para evitar a detecção.

Recomendações de correção:

Se o usuário relatado na descoberta abaixo da `KubernetesUserDetails` seção é `system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogar as permissões, se necessário, seguindo as instruções nas melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom

Uma API foi invocada a partir de um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: alta

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação de API foi invocada a partir de um endereço IP incluído em uma lista de ameaças que você carregou. A lista de ameaças associada a essa descoberta está listada na seção Informações adicionais dos detalhes de uma descoberta. Comumente, a API observada é associada a táticas de evasão de defesa, nas quais um adversário está tentando esconder suas ações para evitar a detecção.

Recomendações de correção:

Se o usuário relatado na descoberta abaixo da `KubernetesUserDetails` seção é `system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogar as permissões, se necessário, seguindo as instruções nas melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado,

investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess

Uma API comumente usada para evitar medidas defensivas foi invocada por um usuário não autenticado.

Gravidade padrão: alta

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação de API foi invocada com sucesso pelo usuário `system:anonymous`. As chamadas de API feitas por `system:anonymous` não são autenticadas. Comumente, a API observada é associada a táticas de evasão de defesa, nas quais um adversário está tentando esconder suas ações para evitar a detecção. Essa atividade indica que o acesso anônimo ou não autenticado é permitido na ação da API relatada na descoberta e pode ser permitido em outras ações. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais estão comprometidas.

Recomendações de correção:

Você deve examinar as permissões que foram concedidas ao usuário `system:anonymous` em seu cluster e garantir que todas as permissões sejam necessárias. Se as permissões foram concedidas por engano ou de maneira mal-intencionada, você deve revogar o acesso do usuário e reverter as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS.

Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

DefenseEvasion:Kubernetes/TorIPCaller

Uma API comumente usada para evitar medidas defensivas foi invocada a partir de um endereço IP do nó de saída do Tor.

Gravidade padrão: alta

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação da API foi invocada a partir de um endereço IP do nó de saída do Tor. Comumente, a API observada é associada a táticas de evasão de defesa, nas quais um adversário está tentando esconder suas ações para evitar a detecção. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar um acesso não autorizado aos seu cluster do Kubernetes com a intenção de ocultar a verdadeira identidade do invasor.

Recomendações de correção:

Se o usuário relatado na descoberta abaixo da `KubernetesUserDetails` seção é`system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogar as permissões, se necessário, seguindo as instruções nas melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Discovery:Kubernetes/MaliciousIPCaller

Uma API comumente usada para descobrir recursos em um cluster do Kubernetes foi invocada a partir de um endereço IP.

Gravidade padrão: média

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação de API foi invocada a partir de um endereço IP associado a atividades mal-intencionadas conhecidas. Comumente, a API observada é usada no estágio de descoberta de um ataque, no qual um invasor coleta informações para determinar se seu cluster do Kubernetes é suscetível a um ataque mais amplo.

Recomendações de correção:

Se o usuário relatado na descoberta abaixo da `KubernetesUserDetails` seção `ésystem:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogar as permissões, se necessário, seguindo as instruções nas melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Discovery:Kubernetes/MaliciousIPCaller.Custom

Uma API comumente usada para descobrir recursos em um cluster do Kubernetes foi invocada a partir de um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: média

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação da API foi invocada de um endereço IP incluído em uma lista de ameaças que você enviou. A lista de ameaças associada a essa descoberta está listada na seção Informações adicionais dos detalhes de uma descoberta. Comumente, a API observada é usada no estágio de descoberta de um ataque, no qual um invasor coleta informações para determinar se seu cluster do Kubernetes é suscetível a um ataque mais amplo.

Recomendações de correção:

Se o usuário relatado na descoberta abaixo da `KubernetesUserDetails` seção `ésystem:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogar as permissões, se necessário, seguindo as instruções nas melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Discovery:Kubernetes/SuccessfulAnonymousAccess

Uma API comumente usada para descobrir recursos em um cluster do Kubernetes foi invocada por um usuário não autenticado.

Gravidade padrão: média

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação de API foi invocada com sucesso pelo usuário `system:anonymous`. As chamadas de API feitas por `system:anonymous` não são autenticadas. Comumente, a API observada é associada ao estágio de descoberta de um ataque quando um adversário está coletando informações em seu cluster do Kubernetes. Essa atividade indica que o acesso anônimo ou não autenticado é permitido na ação da API relatada na descoberta e pode ser permitido em outras ações. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais estão comprometidas.

Recomendações de correção:

Você deve examinar as permissões que foram concedidas ao usuário `system:anonymous` em seu cluster e garantir que todas as permissões sejam necessárias. Se as permissões foram concedidas por engano ou de maneira mal-intencionada, você deve revogar o acesso do usuário e reverter as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS.

Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Discovery:Kubernetes/TorIPCaller

Uma API comumente usada para descobrir recursos em um cluster do Kubernetes foi invocada a partir de um endereço IP do nó de saída do Tor.

Gravidade padrão: média

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação da API foi invocada a partir de um endereço IP do nó de saída do Tor. Comumente, a API observada é usada no estágio de descoberta de um ataque, no qual um invasor coleta informações para determinar se seu cluster do Kubernetes é suscetível a um ataque mais amplo. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar um acesso não autorizado aos seu cluster do Kubernetes com a intenção de ocultar a verdadeira identidade do invasor.

Recomendações de correção:

Se o usuário relatado na descoberta na `KubernetesUserDetails` seção é`system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogar as permissões, se necessário, seguindo as instruções nas melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Execution:Kubernetes/ExecInKubeSystemPod

Um comando foi executado dentro de um pod no namespace **`kube-system`**

Gravidade padrão: média

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que um comando foi executado em um pod dentro do namespace `kube-system` usando a API Kubernetes exec. O namespace `kube-system` é padrão, usado principalmente para componentes de nível de sistema, como `kube-dns` e `kube-proxy`. É muito incomum executar comandos dentro de pods ou contêineres no namespace `kube-system` e pode indicar atividade suspeita.

Recomendações de correção:

Se a execução desse comando for inesperada, as credenciais da identidade do usuário usadas para executar o comando poderão ser comprometidas. Revogue o acesso do usuário e reverta todas as alterações feitas por um adversário em seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Impact:Kubernetes/MaliciousIPCaller

Uma API comumente usada para adulterar recursos em um cluster do Kubernetes foi invocada a partir de um endereço IP mal-intencionado conhecido.

Gravidade padrão: alta

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação de API foi invocada a partir de um endereço IP associado a atividades mal-intencionadas conhecidas. A API observada é comumente associada a táticas de impacto em que um adversário está tentando manipular, interromper ou destruir dados em seu ambiente. AWS

Recomendações de correção:

Se o usuário relatado na descoberta abaixo da `KubernetesUserDetails` seção é`system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogar as permissões, se necessário, seguindo as instruções nas melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Impact:Kubernetes/MaliciousIPCaller.Custom

Uma API comumente usada para adulterar recursos em um cluster do Kubernetes foi invocada a partir de um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: alta

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação de API foi invocada a partir de um endereço IP incluído em uma lista de ameaças que você carregou. A lista de ameaças associada a essa descoberta está listada na seção Informações adicionais dos detalhes de uma descoberta. A API observada

é comumente associada a táticas de impacto em que um adversário está tentando manipular, interromper ou destruir dados em seu ambiente. AWS

Recomendações de correção:

Se o usuário relatado na descoberta abaixo da `KubernetesUserDetails` seção é`system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogar as permissões, se necessário, seguindo as instruções nas melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Impact:Kubernetes/SuccessfulAnonymousAccess

Uma API comumente usada para adulterar recursos em um cluster do Kubernetes foi invocada por um usuário não autenticado.

Gravidade padrão: alta

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação de API foi invocada com sucesso pelo usuário `system:anonymous`. As chamadas de API feitas por `system:anonymous` não são autenticadas. Comumente, a API observada é associada ao estágio de impacto de um ataque quando um adversário está adulterando recursos em seu cluster. Essa atividade indica que o acesso anônimo ou não autenticado é permitido na ação da API relatada na descoberta e pode ser permitido em outras ações. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais estão comprometidas.

Recomendações de correção:

Você deve examinar as permissões que foram concedidas ao usuário `system:anonymous` em seu cluster e garantir que todas as permissões sejam necessárias. Se as permissões foram concedidas por engano ou de maneira mal-intencionada, você deve revogar o acesso do usuário e reverter as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS.

Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Impact:Kubernetes/TorIPCaller

Uma API comumente usada para adulterar recursos em um cluster do Kubernetes foi invocada a partir de um endereço IP do nó de saída do Tor.

Gravidade padrão: alta

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação da API foi invocada a partir de um endereço IP do nó de saída do Tor. Comumente, a API observada é associada a táticas de impacto em que um adversário está tentando manipular, interromper ou destruir dados em seu ambiente da AWS . Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar um acesso não autorizado aos seu cluster do Kubernetes com a intenção de ocultar a verdadeira identidade do invasor.

Recomendações de correção:

Se o usuário relatado na descoberta abaixo da `KubernetesUserDetails` seção é`system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogar as permissões, se necessário, seguindo as instruções nas melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Persistence:Kubernetes/ContainerWithSensitiveMount

Um contêiner foi lançado com um caminho de host externo sensível montado em seu interior.

Gravidade padrão: média

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que um contêiner foi lançado com uma configuração que incluía um caminho de host confidencial com acesso de gravação na seção `volumeMounts`. Isso torna o caminho confidencial do host acessível e gravável de dentro do contêiner. Essa técnica é comumente usada por adversários para obter acesso ao sistema de arquivos do host.

Recomendações de correção:

Se o lançamento desse contêiner for inesperado, as credenciais da identidade do usuário usadas para iniciar o contêiner poderão ser comprometidas. Revogue o acesso do usuário e reverta todas as alterações feitas por um adversário em seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Se o lançamento desse contêiner for esperado, é recomendável usar uma regra de supressão que consiste em um critério de filtro com base no campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nos critérios de filtro, o campo `imagePrefix` deve ser o mesmo que o `imagePrefix` especificado na descoberta. Para saber mais sobre a criação de regras de supressão, consulte Regras de supressão.

Persistence:Kubernetes/MaliciousIPCaller

Uma API comumente usada para obter acesso persistente a um cluster do Kubernetes foi invocada a partir de um endereço IP mal-intencionado conhecido.

Gravidade padrão: média

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação de API foi invocada a partir de um endereço IP associado a atividades mal-intencionadas conhecidas. Comumente, a API observada é associada a táticas de persistência em que um adversário obteve acesso ao seu cluster do Kubernetes e está tentando manter esse acesso.

Recomendações de correção:

Se o usuário relatado na descoberta abaixo da `KubernetesUserDetails` seção `ésystem:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogar as permissões, se necessário, seguindo as instruções nas melhores práticas de segurança

para o Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Persistence:Kubernetes/MaliciousIPCaller.Custom

Uma API comumente usada para obter acesso persistente a um cluster do Kubernetes foi invocada a partir de um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: média

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação de API foi invocada a partir de um endereço IP incluído em uma lista de ameaças que você carregou. A lista de ameaças associada a essa descoberta está listada na seção Informações adicionais dos detalhes de uma descoberta. Comumente, a API observada é associada a táticas de persistência em que um adversário obteve acesso ao seu cluster do Kubernetes e está tentando manter esse acesso.

Recomendações de correção:

Se o usuário relatado na descoberta abaixo da `KubernetesUserDetails` seção é `system:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogar as permissões, se necessário, seguindo as instruções nas melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Persistence:Kubernetes/SuccessfulAnonymousAccess

Uma API comumente usada para obter permissões de alto nível para um cluster do Kubernetes foi invocada por um usuário não autenticado.

Gravidade padrão: alta

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação de API foi invocada com sucesso pelo usuário `system:anonymous`. As chamadas de API feitas por `system:anonymous` não são autenticadas. Comumente, a API observada é associada às táticas de persistência em que um adversário obteve acesso ao seu cluster e está tentando manter esse acesso. Essa atividade indica que o acesso anônimo ou não autenticado é permitido na ação da API relatada na descoberta e pode ser permitido em outras ações. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais estão comprometidas.

Recomendações de correção:

Você deve examinar as permissões que foram concedidas ao usuário `system:anonymous` em seu cluster e garantir que todas as permissões sejam necessárias. Se as permissões foram concedidas por engano ou de maneira mal-intencionada, você deve revogar o acesso do usuário e reverter as alterações feitas por um adversário no seu cluster. Para obter mais informações, consulte Melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS.

Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Persistence:Kubernetes/TorIPCaller

Uma API comumente usada para obter acesso persistente a um cluster do Kubernetes foi invocada a partir de um endereço IP do nó de saída do Tor.

Gravidade padrão: média

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação da API foi invocada a partir de um endereço IP do nó de saída do Tor. Comumente, a API observada é associada a táticas de persistência em que um adversário obteve acesso ao seu cluster do Kubernetes e está tentando manter esse acesso. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar acesso não autorizado aos seus AWS recursos com a intenção de ocultar a verdadeira identidade do atacante.

Recomendações de correção:

Se o usuário relatado na descoberta abaixo da `KubernetesUserDetails` seção `ésystem:anonymous`, investigue por que o usuário anônimo teve permissão para invocar a API e revogar as permissões, se necessário, seguindo as instruções nas melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS. Se o usuário for um usuário autenticado, investigue para determinar se a atividade foi legítima ou mal-intencionada. Se a atividade for mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um adversário no seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Policy:Kubernetes/AdminAccessToDefaultServiceAccount

A conta de serviço padrão recebeu privilégios de administrador em um cluster do Kubernetes.

Gravidade padrão: alta

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que a conta de serviço padrão de um namespace em seu cluster do Kubernetes recebeu privilégios de administrador. O Kubernetes cria uma conta de serviço padrão para todos os namespaces no cluster. Ele atribui automaticamente a conta de serviço padrão como uma identidade aos pods que não foram explicitamente associados a outra conta de serviço. Se a conta de serviço padrão tiver privilégios de administrador, isso poderá resultar no lançamento involuntário de pods com privilégios de administrador. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais estão comprometidas.

Recomendações de correção:

Não use a conta de serviço padrão para conceder permissões aos pods. Em vez disso, você deve criar uma conta de serviço dedicada para cada workload e conceder permissão a essa conta de acordo com as necessidades. Para corrigir esse problema, você deve criar contas de serviço dedicadas para todos os seus pods e workloads e atualizar os pods e workloads para migrar da conta de serviço padrão para suas contas dedicadas. Em seguida, é necessário remover a permissão de administrador da conta de serviço padrão. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Policy:Kubernetes/AnonymousAccessGranted

O usuário **`system:anonymous`** recebeu permissão de API em um cluster do Kubernetes.

Gravidade padrão: alta

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que um usuário em seu cluster do Kubernetes criou com sucesso um `ClusterRoleBinding` ou `RoleBinding` para vincular o usuário `system:anonymous` a um perfil. Isso permite acesso não autenticado às operações de API permitidas pelo perfil. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais estão comprometidas

Recomendações de correção:

Você deve examinar as permissões que foram concedidas ao usuário `system:anonymous` ou grupo `system:unauthenticated` em seu cluster e revogar o acesso anônimo desnecessário. Para obter mais informações, consulte Melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS. Se as permissões foram concedidas de maneira mal-intencionada, você deve revogar o acesso do usuário que concedeu as permissões e reverter quaisquer alterações feitas por um adversário em seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Policy:Kubernetes/ExposedDashboard

O painel de um cluster do Kubernetes foi exposto à Internet

Gravidade padrão: média

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que o painel do Kubernetes do seu cluster foi exposto à Internet por um serviço de balanceador de carga. Um painel exposto torna a interface de gerenciamento do seu cluster acessível pela Internet e permite que os adversários explorem quaisquer lacunas de autenticação e controle de acesso que possam estar presentes.

Recomendações de correção:

Você deve garantir que a autenticação e a autorização fortes sejam aplicadas no Painel do Kubernetes. Você também deve implementar o controle de acesso à rede para restringir o acesso ao painel a partir de endereços IP específicos.

Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Policy:Kubernetes/KubeflowDashboardExposed

O painel Kubeflow de um cluster do Kubernetes foi exposto à Internet

Gravidade padrão: média

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que o painel Kubeflow do seu cluster foi exposto à Internet por um serviço de balanceador de carga. Um painel exposto do Kubeflow torna a interface de gerenciamento do seu ambiente Kubeflow acessível pela Internet e permite que os adversários explorem quaisquer lacunas de autenticação e controle de acesso que possam estar presentes.

Recomendações de correção:

Você deve garantir que a autenticação e a autorização fortes sejam aplicadas no Painel Kubeflow. Você também deve implementar o controle de acesso à rede para restringir o acesso ao painel a partir de endereços IP específicos.

Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

PrivilegeEscalation:Kubernetes/PrivilegedContainer

Um contêiner privilegiado com acesso de nível raiz foi lançado em seu cluster do Kubernetes.

Gravidade padrão: média

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que um contêiner privilegiado foi lançado em seu cluster do Kubernetes usando uma imagem nunca antes usada para iniciar contêineres privilegiados em seu cluster. Um contêiner privilegiado tem acesso de nível raiz ao host. Os adversários podem lançar contêineres privilegiados como uma tática de escalonamento de privilégios para obter acesso e, em seguida, comprometer o host.

Recomendações de correção:

Se o lançamento desse contêiner for inesperado, as credenciais da identidade do usuário usadas para iniciar o contêiner poderão ser comprometidas. Revogue o acesso do usuário e reverta todas as alterações feitas por um adversário em seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed

Uma API do Kubernetes comumente usada para acessar segredos foi invocada de forma anômala.

Gravidade padrão: média

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação anômala de API para recuperar segredos confidenciais do cluster foi invocada por um usuário do Kubernetes em seu cluster. Comumente, a API observada é associada a táticas de acesso a credenciais que podem levar a um escalonamento privilegiado e a um maior acesso ao seu cluster. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas AWS credenciais estão comprometidas.

A API observada foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todas as atividades da API do usuário em seu cluster do EKS e identifica eventos anômalos associados a técnicas usadas por usuários não autorizados. O modelo de ML rastreia vários fatores da operação da API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, o agente do usuário usado e o namespace que o usuário operou. Você pode encontrar os detalhes incomuns da solicitação de API no painel de busca de detalhes no GuardDuty console.

Recomendações de correção:

Examine as permissões concedidas ao usuário do Kubernetes em seu cluster e garanta que todas essas permissões sejam necessárias. Se as permissões foram concedidas por engano ou de maneira mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um usuário não autorizado em seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Se suas AWS credenciais estiverem comprometidas, consulte. Correção de credenciais potencialmente comprometidas AWS

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated

Um RoleBinding ou ClusterRoleBinding para um papel excessivamente permissivo ou namespace confidencial foi criado ou modificado em seu cluster Kubernetes.

Gravidade padrão: média*

> **Note**
>
> A gravidade padrão desta descoberta é Média. No entanto, se um RoleBinding ou ClusterRoleBinding envolver o ClusterRoles `admin` ou`cluster-admin`, a gravidade será Alta.

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que um usuário em seu cluster do Kubernetes criou um `RoleBinding` ou `ClusterRoleBinding` para vincular um usuário a uma função com permissões de administrador ou namespaces confidenciais. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas AWS credenciais estão comprometidas.

A API observada foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todas as atividades da API do usuário em seu cluster do EKS. Esse modelo de ML também identifica eventos anômalos associados às técnicas usadas por um usuário não autorizado. O modelo de ML também rastreia vários fatores da operação da API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, o agente do usuário usado e o namespace que o usuário operou. Você pode encontrar os detalhes incomuns da solicitação de API no painel de busca de detalhes no GuardDuty console.

Recomendações de correção:

Examine as permissões concedidas ao usuário do Kubernetes. Essas permissões são definidas na função e nos assuntos envolvidos em `RoleBinding` e `ClusterRoleBinding`. Se as permissões foram concedidas por engano ou de maneira mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um usuário não autorizado em seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Se suas AWS credenciais estiverem comprometidas, consulte. Correção de credenciais potencialmente comprometidas AWS

Execution:Kubernetes/AnomalousBehavior.ExecInPod

Um comando foi executado dentro de um pod de forma anômala.

Gravidade padrão: média

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que um comando foi executado em um pod usando a API Kubernetes exec. A API Kubernetes exec permite executar comandos arbitrários em um pod. Se esse comportamento não for esperado para o usuário, namespace ou pod, isso pode indicar um erro de configuração ou que suas AWS credenciais estão comprometidas.

A API observada foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todas as atividades da API do usuário em seu cluster do EKS. Esse modelo de ML também identifica eventos anômalos associados às técnicas usadas por um usuário não autorizado. O modelo de ML também rastreia vários fatores da operação da API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, o agente do usuário usado e o namespace que o usuário operou. Você pode encontrar os detalhes incomuns da solicitação de API no painel de busca de detalhes no GuardDuty console.

Recomendações de correção:

Se a execução desse comando for inesperada, as credenciais da identidade do usuário usadas para executar o comando podem ter sido comprometidas. Revogue o acesso do usuário e reverta todas as alterações feitas por um usuário não autorizado em seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Se suas AWS credenciais estiverem comprometidas, consulte. Correção de credenciais potencialmente comprometidas AWS

PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer

Uma workload foi lançada com um contêiner privilegiado de forma anômala.

Gravidade padrão: alta

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma workload foi lançada com um contêiner privilegiado em seu cluster Amazon EKS. Um contêiner privilegiado tem acesso de nível raiz ao host. Usuários não autorizados podem lançar contêineres privilegiados como uma tática de escalonamento de privilégios para primeiro obter acesso ao host e depois comprometê-lo.

A criação ou modificação observada do contêiner foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todas as atividades da API do usuário e da imagem do contêiner em seu cluster do EKS. Esse modelo de ML também identifica eventos anômalos associados às técnicas usadas por um usuário não autorizado. O modelo de ML também rastreia vários fatores da operação da API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, o agente do usuário usado, as imagens de contêiner observadas em sua conta e o namespace operado pelo usuário. Você pode encontrar os detalhes incomuns da solicitação de API no painel de busca de detalhes no GuardDuty console.

Recomendações de correção:

Se o lançamento desse contêiner for inesperado, as credenciais da identidade do usuário usadas para iniciar o contêiner podem ter sido comprometidas. Revogue o acesso do usuário e reverta todas as alterações feitas por um usuário não autorizado em seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Se suas AWS credenciais estiverem comprometidas, consulte. Correção de credenciais potencialmente comprometidas AWS

Se o lançamento desse contêiner for esperado, é recomendável usar uma regra de supressão com um critério de filtro baseado no campo

`resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nos critérios de filtro, o campo `imagePrefix` deve ter o mesmo valor do campo `imagePrefix` especificado na descoberta. Para ter mais informações, consulte Regras de supressão.

Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed! ContainerWithSensitiveMount

Uma workload foi implantada de forma anômala, com um caminho de host sensível montado dentro da workload.

Gravidade padrão: alta

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma workload foi lançada com um contêiner que incluía um caminho de host confidencial na seção `volumeMounts`. Isso potencialmente torna o caminho confidencial do host acessível e gravável de dentro do contêiner. Essa técnica é comumente usada por usuários não autorizados para obter acesso ao sistema de arquivos do host.

A criação ou modificação observada do contêiner foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todas as atividades da API do usuário e da imagem do contêiner em seu cluster do EKS. Esse modelo de ML também identifica eventos anômalos associados às técnicas usadas por um usuário não autorizado. O modelo de ML também rastreia vários fatores da operação da API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, o agente do usuário usado, as imagens de contêiner observadas em sua conta e o namespace operado pelo usuário. Você pode encontrar os detalhes incomuns da solicitação de API no painel de busca de detalhes no GuardDuty console.

Recomendações de correção:

Se o lançamento desse contêiner for inesperado, as credenciais da identidade do usuário usadas para iniciar o contêiner podem ter sido comprometidas. Revogue o acesso do usuário e reverta todas as alterações feitas por um usuário não autorizado em seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Se suas AWS credenciais estiverem comprometidas, consulte. Correção de credenciais potencialmente comprometidas AWS

Se o lançamento desse contêiner for esperado, é recomendável usar uma regra de supressão com um critério de filtro baseado no campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nos critérios de filtro, o campo `imagePrefix` deve ter o mesmo valor do campo `imagePrefix` especificado na descoberta. Para ter mais informações, consulte Regras de supressão.

Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed

Uma workload foi lançada de forma anômala.

Gravidade padrão: baixa*

> **Note**
>
> A gravidade padrão é Baixa. No entanto, se a workload contiver um nome de imagem potencialmente suspeito, como uma ferramenta de teste de penetração conhecida, ou um contêiner executando um comando potencialmente suspeito na inicialização, como comandos de shell reverso, a gravidade desse tipo de descoberta será considerada Média.

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma workload do Kubernetes foi criada ou modificada de forma anômala, como uma atividade de API, novas imagens de contêiner ou configuração de workload arriscada, dentro do seu cluster Amazon EKS. Usuários não autorizados podem lançar contêineres como uma tática para executar código arbitrário para primeiro obter acesso ao host e depois comprometê-lo.

A criação ou modificação observada do contêiner foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todas as atividades da API do usuário e da imagem do contêiner em seu cluster do EKS. Esse modelo de ML também identifica eventos anômalos associados às técnicas usadas por um usuário não autorizado. O modelo de ML também rastreia vários fatores da operação da API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, o agente do usuário usado, as imagens de contêiner observadas em sua conta e o namespace operado pelo usuário. Você pode encontrar os detalhes incomuns da solicitação de API no painel de busca de detalhes no GuardDuty console.

Recomendações de correção:

Se o lançamento desse contêiner for inesperado, as credenciais da identidade do usuário usadas para iniciar o contêiner podem ter sido comprometidas. Revogue o acesso do usuário e reverta todas as alterações feitas por um usuário não autorizado em seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Se suas AWS credenciais estiverem comprometidas, consulte. Correção de credenciais potencialmente comprometidas AWS

Se o lançamento desse contêiner for esperado, é recomendável usar uma regra de supressão com um critério de filtro baseado no campo `resource.KubernetesDetails.KubernetesWorkloadDetails.containers.imagePrefix`. Nos critérios de filtro, o campo `imagePrefix` deve ter o mesmo valor do campo `imagePrefix` especificado na descoberta. Para ter mais informações, consulte Regras de supressão.

PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated

Uma função altamente permissiva ou ClusterRole foi criada ou modificada de forma anômala.

Gravidade padrão: baixa

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que uma operação de API anômala para criar `Role` ou `ClusterRole` com permissões excessivas foi chamada por um usuário do Kubernetes em seu cluster Amazon EKS. Os atores podem usar a criação de funções com permissões poderosas para evitar o uso de funções internas semelhantes às de administrador e evitar a detecção. As permissões excessivas podem levar a escalonamento privilegiado, execução remota de código e, potencialmente, controle sobre um namespace ou cluster. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais estão comprometidas.

A API observada foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todas as atividades de API do usuário em seu cluster Amazon EKS e identifica eventos anômalos associados às técnicas usadas por usuários não autorizados. O modelo de ML também rastreia vários fatores da operação da API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, o agente do usuário usado, as

imagens de contêiner observadas em sua conta e o namespace operado pelo usuário. Você pode encontrar os detalhes incomuns da solicitação de API no painel de busca de detalhes no GuardDuty console.

Recomendações de correção:

Examine as permissões definidas em `Role` ou `ClusterRole` para garantir que todas as permissões sejam necessárias e siga os princípios de privilégios mínimos. Se as permissões foram concedidas por engano ou de maneira mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um usuário não autorizado em seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Se suas AWS credenciais estiverem comprometidas, consulte. Correção de credenciais potencialmente comprometidas AWS

Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

Um usuário verificou sua permissão de acesso de forma anômala.

Gravidade padrão: baixa

- Atributo: logs de auditoria do Kubernetes

Essa descoberta informa que um usuário em seu cluster do Kubernetes verificou com sucesso se as poderosas permissões conhecidas que podem levar ao escalonamento privilegiado e à execução remota de código são permitidas. Por exemplo, um comando comum usado para verificar as permissões de um usuário é `kubectl auth can-i`. Se esse comportamento não for esperado, isso pode indicar um erro de configuração ou que suas credenciais foram comprometidas.

A API observada foi identificada como anômala pelo modelo de aprendizado de máquina (ML) de detecção de GuardDuty anomalias. O modelo de ML avalia todas as atividades de API do usuário em seu cluster Amazon EKS e identifica eventos anômalos associados às técnicas usadas por usuários não autorizados. O modelo de ML também rastreia vários fatores da operação da API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, a permissão que está sendo verificada e o namespace que o usuário operou. Você pode encontrar os detalhes incomuns da solicitação de API no painel de busca de detalhes no GuardDuty console.

Recomendações de correção:

Examine as permissões concedidas ao usuário do Kubernetes para garantir que todas as permissões sejam necessárias. Se as permissões foram concedidas por engano ou de maneira mal-intencionada, revogue o acesso do usuário e reverta as alterações feitas por um usuário não autorizado em seu cluster. Para ter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Se suas AWS credenciais estiverem comprometidas, consulte. Correção de credenciais potencialmente comprometidas AWS

Tipos de descoberta do Lambda Protection

Esta seção descreve os tipos de descoberta que são específicos de seus AWS Lambda recursos e estão `resourceType` listados como`Lambda`. Para todas as descobertas do Lambda, recomendamos que você examine o recurso em questão e determine se ele está se comportando da maneira esperada. Se a atividade for autorizada, você poderá usar regras de supressão ou listas de IPs confiáveis e de ameaças para evitar notificações de falsos positivos para esse recurso.

Se a atividade for inesperada, a melhor prática de segurança é presumir que o Lambda foi potencialmente comprometido e seguir as recomendações de remediação.

Tópicos

- Backdoor:Lambda/C&CActivity.B
- CryptoCurrency:Lambda/BitcoinTool.B
- Trojan:Lambda/BlackholeTraffic
- Trojan:Lambda/DropPoint
- UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom
- UnauthorizedAccess:Lambda/TorClient
- UnauthorizedAccess:Lambda/TorRelay

Backdoor:Lambda/C&CActivity.B

Uma função do Lambda está consultando um endereço IP associado a um servidor de comando e controle conhecido.

Severidade padrão: alta

- Atributo: Monitoramento de atividades de rede do Lambda

Essa descoberta informa que uma função do Lambda listada em seu ambiente da AWS está consultando um endereço IP associado a um servidor conhecido de comando e controle (C&C). A função do Lambda associada à descoberta gerada está potencialmente comprometida. Os servidores C&C são computadores que enviam comandos para membros de um botnet.

Um botnet é uma coleção de dispositivos conectados à Internet (que podem incluir PCs, servidores, dispositivos móveis e dispositivos de Internet das Coisas) infectados e controlados por um tipo comum de malware. Os botnets são frequentemente usados para distribuir malwares e coletar informações inapropriadas, como números de cartão de crédito. Dependendo da finalidade e da estrutura do botnet, o servidor C&C também pode emitir comandos para iniciar um ataque de negação distribuída de serviço DDoS.

Recomendações de correção:

Se essa atividade for inesperada, sua função do Lambda pode estar comprometida. Para obter mais informações, consulte Correção de uma função Lambda potencialmente comprometida.

CryptoCurrency:Lambda/BitcoinTool.B

Uma função do Lambda está consultando um endereço IP associado à atividade relacionada a uma criptomoeda.

Severidade padrão: alta

- Atributo: Monitoramento de atividades de rede do Lambda

Essa descoberta informa a você que uma função do Lambda em seu ambiente da AWS está consultando um endereço IP associado à Bitcoin ou a atividades relacionadas a outras criptomoedas. Os agentes de ameaças podem tentar assumir o controle das funções do Lambda para redirecioná-las maliciosamente para a mineração não autorizada de criptomoedas.

Recomendações de correção:

Se você usa essa função do Lambda para minerar ou gerenciar criptomoedas, ou se essa função estiver envolvida em uma atividade de blockchain, ela é potencialmente uma atividade esperada para seu ambiente. Se esse for o caso em seu ambiente da AWS, recomendamos configurar uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de

CryptoCurrency:Lambda/BitcoinTool.B. O segundo critério de filtro deve ser o nome da função do Lambda da função envolvida na atividade do blockchain. Para obter informações sobre a criação de regras de supressão, consulte Regras de supressão.

Se essa atividade for inesperada, sua função do Lambda está potencialmente comprometida. Para obter mais informações, consulte Correção de uma função Lambda potencialmente comprometida.

Trojan:Lambda/BlackholeTraffic

A função do Lambda está tentando se comunicar com um endereço IP de um host remoto que é um buraco negro conhecido.

Severidade padrão: média

- Atributo: Monitoramento de atividades de rede do Lambda

Essa descoberta informa que uma função do Lambda listada em AWS seu ambiente está tentando se comunicar com o endereço IP de um buraco negro (ou sumidouro). Os buracos negros são locais na rede onde o tráfego de entrada ou de saída é descartado silenciosamente sem informar a fonte de que os dados não atingiram o destinatário pretendido. Um endereço IP de buraco negro especifica uma máquina host que não está sendo executada ou um endereço para o qual nenhum host foi atribuído. A função do Lambda listada está potencialmente comprometida.

Recomendações de correção:

Se essa atividade for inesperada, sua função do Lambda pode estar comprometida. Para obter mais informações, consulte Correção de uma função Lambda potencialmente comprometida.

Trojan:Lambda/DropPoint

Uma função do Lambda está tentando se comunicar com um endereço IP de um host remoto que é conhecido por manter credenciais e outros dados roubados capturados por malware.

Severidade padrão: média

- Atributo: Monitoramento de atividades de rede do Lambda

Essa descoberta informa que uma função do Lambda listada em seu ambiente da AWS está tentando se comunicar com um endereço IP de um host remoto que é conhecido por manter credenciais e outros dados roubados capturados por malware.

Recomendações de correção:

Se essa atividade for inesperada, sua função do Lambda pode estar comprometida. Para obter mais informações, consulte Correção de uma função Lambda potencialmente comprometida.

UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom

Uma função do Lambda está fazendo conexões com um endereço IP em uma lista de ameaças personalizada.

Severidade padrão: média

- Atributo: Monitoramento de atividades de rede do Lambda

Essa descoberta informa que uma função do Lambda no seu ambiente da AWS está se comunicando por meio de um endereço IP incluído em uma lista de ameaças que você carregou. No GuardDuty, uma lista de ameaças consiste em endereços IP maliciosos conhecidos. O GuardDuty gera descobertas com base nas listas de ameaças carregadas. Você pode ver os detalhes da lista de ameaças nos detalhes da descoberta no console do GuardDuty.

Recomendações de correção:

Se essa atividade for inesperada, sua função do Lambda pode estar comprometida. Para obter mais informações, consulte Correção de uma função Lambda potencialmente comprometida.

UnauthorizedAccess:Lambda/TorClient

A função do Lambda está fazendo conexões com um Tor Guard ou um nó de autoridade.

Severidade padrão: alta

- Atributo: Monitoramento de atividades de rede do Lambda

Essa descoberta informa que uma função do Lambda em seu ambiente da AWS está fazendo conexões com um Tor Guard ou um nó de autoridade. Tor é um software para permitir a comunicação anônima. Tor Guards ou nós de autoridade atuam como gateways iniciais em uma rede do Tor. Esse tráfego pode indicar que essa função do Lambda foi potencialmente comprometida. Agora ele está atuando como um cliente em uma rede Tor.

Recomendações de correção:

Se essa atividade for inesperada, sua função do Lambda pode estar comprometida. Para obter mais informações, consulte Correção de uma função Lambda potencialmente comprometida.

UnauthorizedAccess:Lambda/TorRelay

Uma função do Lambda está fazendo conexões com uma rede Tor como uma retransmissão Tor.

Severidade padrão: alta

- Atributo: Monitoramento de atividades de rede do Lambda

Essa descoberta informa que uma função do Lambda em seu ambiente da AWS está fazendo conexões com uma rede Tor de uma maneira que sugere que ela está agindo como um retransmissor Tor. Tor é um software para permitir a comunicação anônima. O Tor habilita a comunicação anônima encaminhando tráfego potencialmente ilícito do cliente de uma retransmissão Tor para outra.

Recomendações de correção:

Se essa atividade for inesperada, sua função do Lambda pode estar comprometida. Para obter mais informações, consulte Correção de uma função Lambda potencialmente comprometida.

Tipos de descoberta de Malware Protection

A Proteção contra malware do GuardDuty fornece uma única descoberta de Proteção contra malware para todas as ameaças detectadas durante a verificação de uma instância do EC2 ou de uma workload de contêiner. A descoberta inclui o número total de detecções feitas durante a verificação e, com base na gravidade, fornece detalhes das 32 principais ameaças detectadas.

Diferentemente de outras descobertas do GuardDuty, as descobertas do Malware Protection não são atualizadas quando a mesma instância do EC2 ou workload do contêiner é verificada novamente.

Uma nova descoberta de Malware Protection é gerada para cada verificação que detecta malware. As descobertas da Malware Protection incluem informações sobre a verificação correspondente que produziu a descoberta, bem como a descoberta do GuardDuty que iniciou essa verificação. Isso facilita a correlação do comportamento suspeito com o malware detectado.

> **Note**
>
> Quando o GuardDuty detecta atividades maliciosas em uma workload de contêiner, o Malware Protection não gera uma descoberta no nível do EC2.

As descobertas a seguir são específicas do Proteção contra malware do GuardDuty.

Tópicos

Execution:EC2/MaliciousFile

Um arquivo malicioso foi detectado em uma instância do EC2.

Severidade padrão: varia de acordo com a ameaça detectada.

Essa descoberta indica que a verificação do Proteção contra malware do GuardDuty detectou um ou mais arquivos maliciosos na instância do EC2 listada em seu ambiente. AWS Essa instância listada pode estar comprometida. Para obter mais informações, consulte a seção Ameaças detectadas nos detalhes das descobertas.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Execution:ECS/MaliciousFile

Um arquivo malicioso foi detectado em um cluster do ECS.

Severidade padrão: varia de acordo com a ameaça detectada.

Essa descoberta indica que a verificação do Proteção contra malware do GuardDuty detectou um ou mais arquivos maliciosos em uma workload de contêiner que pertence a um cluster ECS. Para obter mais informações, consulte a seção Ameaças detectadas nos detalhes das descobertas.

Recomendações de correção:

Se essa atividade for inesperada, seu contêiner pertencente ao cluster ECS poderá ser comprometido. Para obter mais informações, consulte Correção de um cluster ECS potencialmente comprometido.

Execution:Kubernetes/MaliciousFile

Um arquivo malicioso foi detectado em um cluster Kubernetes.

Severidade padrão: varia de acordo com a ameaça detectada.

Essa descoberta indica que a verificação do Proteção contra malware do GuardDuty detectou um ou mais arquivos maliciosos em uma workload de contêiner que pertence a um cluster Kubernetes. Se for um cluster gerenciado pelo EKS, os detalhes das descobertas fornecerão informações adicionais sobre o recurso EKS afetado. Para obter mais informações, consulte a seção Ameaças detectadas nos detalhes das descobertas.

Recomendações de correção:

Se essa atividade for inesperada, a workload do contêiner poderá ser comprometida. Para obter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Execution:Container/MaliciousFile

Um arquivo malicioso foi detectado em um contêiner independente.

Severidade padrão: varia de acordo com a ameaça detectada.

Essa descoberta indica que a verificação do Proteção contra malware do GuardDuty detectou um ou mais arquivos maliciosos na workload de um contêiner e nenhuma informação do cluster foi identificada. Para obter mais informações, consulte a seção Ameaças detectadas nos detalhes das descobertas.

Recomendações de correção:

Se essa atividade for inesperada, a workload do contêiner poderá ser comprometida. Para obter mais informações, consulte Correção de um contêiner autônomo potencialmente comprometido.

Execution:EC2/SuspiciousFile

Um arquivo suspeito foi detectado em uma instância do EC2.

Severidade padrão: varia de acordo com a ameaça detectada.

Essa descoberta indica que a verificação do Proteção contra malware do GuardDuty detectou um ou mais arquivos suspeitos em uma instância do EC2. Para obter mais informações, consulte a seção Ameaças detectadas nos detalhes das descobertas.

As detecções de tipo `SuspiciousFile` indicam que programas potencialmente indesejados, como adware, spyware ou ferramentas de uso duplo, estão presentes em um recurso afetado. Esses programas podem ter um impacto neghabilito em seus recursos ou ser usados por invasores para fins maliciosos. Por exemplo, ferramentas de rede podem ser usadas de forma legítima ou maliciosa por adversários como ferramentas de hack para tentar comprometer recursos.

Quando um arquivo suspeito for detectado, avalie se você espera ver o arquivo detectado em seu AWS ambiente. Se o arquivo for inesperado, siga as recomendações de correção fornecidas na próxima seção.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Execution:ECS/SuspiciousFile

Um arquivo suspeito foi detectado em um cluster ECS.

Severidade padrão: varia de acordo com a ameaça detectada.

Essa descoberta indica que a verificação do Proteção contra malware do GuardDuty detectou um ou mais arquivos suspeitos em um contêiner que pertence a um cluster ECS. Para obter mais informações, consulte a seção Ameaças detectadas nos detalhes das descobertas.

As detecções de tipo `SuspiciousFile` indicam que programas potencialmente indesejados, como adware, spyware ou ferramentas de uso duplo, estão presentes em um recurso afetado. Esses programas podem ter um impacto neghabilito em seus recursos ou ser usados por invasores para fins maliciosos. Por exemplo, ferramentas de rede podem ser usadas de forma legítima ou maliciosa por adversários como ferramentas de hack para tentar comprometer recursos.

Quando um arquivo suspeito for detectado, avalie se você espera ver o arquivo detectado em seu AWS ambiente. Se o arquivo for inesperado, siga as recomendações de correção fornecidas na próxima seção.

Recomendações de correção:

Se essa atividade for inesperada, seu contêiner pertencente ao cluster ECS poderá ser comprometido. Para obter mais informações, consulte Correção de um cluster ECS potencialmente comprometido.

Execution:Kubernetes/SuspiciousFile

Um arquivo suspeito foi detectado em um cluster Kubernetes.

Severidade padrão: varia de acordo com a ameaça detectada.

Essa descoberta indica que a verificação do Proteção contra malware do GuardDuty detectou um ou mais arquivos suspeitos em um contêiner que pertence a um cluster Kubernetes. Se for um cluster gerenciado pelo EKS, os detalhes das descobertas fornecerão informações adicionais sobre o EKS afetado. Para obter mais informações, consulte a seção Ameaças detectadas nos detalhes das descobertas.

As detecções de tipo `SuspiciousFile` indicam que programas potencialmente indesejados, como adware, spyware ou ferramentas de uso duplo, estão presentes em um recurso afetado. Esses programas podem ter um impacto neghabilito em seus recursos ou ser usados por invasores para fins maliciosos. Por exemplo, ferramentas de rede podem ser usadas de forma legítima ou maliciosa por adversários como ferramentas de hack para tentar comprometer recursos.

Quando um arquivo suspeito for detectado, avalie se você espera ver o arquivo detectado em seu AWS ambiente. Se o arquivo for inesperado, siga as recomendações de correção fornecidas na próxima seção.

Recomendações de correção:

Se essa atividade for inesperada, a workload do contêiner poderá ser comprometida. Para obter mais informações, consulte Como corrigir os resultados do Monitoramento de logs de auditoria do EKS.

Execution:Container/SuspiciousFile

Um arquivo suspeito foi detectado em um contêiner independente.

Severidade padrão: varia de acordo com a ameaça detectada.

Essa descoberta indica que a verificação do Proteção contra malware do GuardDuty detectou um ou mais arquivos suspeitos em um contêiner sem informações do cluster. Para obter mais informações, consulte a seção Ameaças detectadas nos detalhes das descobertas.

As detecções de tipo `SuspiciousFile` indicam que programas potencialmente indesejados, como adware, spyware ou ferramentas de uso duplo, estão presentes em um recurso afetado. Esses programas podem ter um impacto neghabilito em seus recursos ou ser usados por invasores para fins maliciosos. Por exemplo, ferramentas de rede podem ser usadas de forma legítima ou maliciosa por adversários como ferramentas de hack para tentar comprometer recursos.

Quando um arquivo suspeito for detectado, avalie se você espera ver o arquivo detectado em seu AWS ambiente. Se o arquivo for inesperado, siga as recomendações de correção fornecidas na próxima seção.

Recomendações de correção:

Se essa atividade for inesperada, a workload do contêiner poderá ser comprometida. Para obter mais informações, consulte Correção de um contêiner autônomo potencialmente comprometido.

Tipos de descoberta do GuardDuty RDS Protection

O GuardDuty RDS Protection detecta um comportamento anômalo de login em sua instância de banco de dados. As descobertas a seguir são específicas do Bancos de dados do Amazon Aurora compatíveis e terão um Tipo de recurso de `RDSDBInstance`. A severidade e os detalhes das descobertas serão diferentes com base no tipo de descoberta.

Tópicos

- CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

- CredentialAccess:RDS/AnomalousBehavior.FailedLogin
- CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce
- CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin
- CredentialAccess:RDS/MaliciousIPCaller.FailedLogin
- Discovery:RDS/MaliciousIPCaller
- CredentialAccess:RDS/TorIPCaller.SuccessfulLogin
- CredentialAccess:RDS/TorIPCaller.FailedLogin
- Discovery:RDS/TorIPCaller

CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin

Um usuário fez login com sucesso em um banco de dados do RDS em sua conta de forma anômala.

Gravidade padrão: Variável

> **Note**
>
> Dependendo do comportamento anômalo associado a essa descoberta, a severidade padrão pode ser Baixa, Média e Alta.
>
> - Baixo — Se o nome de usuário associado a essa descoberta estiver conectado a partir de um endereço IP associado a uma rede privada.
> - Médio — Se o nome de usuário associado a essa descoberta estiver conectado a partir de um endereço IP público.
> - Alto — Se houver um padrão consistente de tentativas de login malsucedidas a partir de endereços IP públicos, indichabilito de políticas de acesso excessivamente permissivas.

- Atributo: monitoramento de atividade de login do RDS

Essa descoberta informa que um login bem-sucedido anômalo foi observado em um banco de dados do RDS em seu ambiente. AWS Isso pode indicar que um usuário invisível anterior fez login em

um banco de dados do RDS pela primeira vez. Um cenário comum é um usuário interno fazendo login em um banco de dados que é acessado programaticamente por aplicativas e não por usuários individuais.

Esse login bem-sucedido foi identificado como anômalo pelo modelo de machine learning (ML) de detecção de anomalias do GuardDuty. O modelo de ML avalia todos os eventos de login do seu banco de dados Bancos de dados do Amazon Aurora compatíveis e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo ML rastreia vários fatores da atividade de login do RDS, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e os detalhes específicos da conexão do banco de dados que foram usados. Para obter informações sobre os eventos de login que são potencialmente incomuns, consulteAnomalias baseadas na atividade de login do RDS.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, é recomendável alterar a senha do usuário do banco de dados associado e revisar os registros de auditoria disponíveis para a atividade realizada pelo usuário anômalo. Descobertas de severidade média e alta podem indicar que há uma política de acesso excessivamente permissiva ao banco de dados e que as credenciais do usuário podem ter sido expostas ou comprometidas. É recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigir um banco de dados potencialmente comprometido com eventos de login bem-sucedidos.

CredentialAccess:RDS/AnomalousBehavior.FailedLogin

Uma ou mais tentativas incomuns de login malsucedidas foram observadas em um banco de dados do RDS em sua conta.

Severidade padrão: baixa

- Atributo: monitoramento de atividade de login do RDS

Essa descoberta informa que um ou mais logins com falha anômala foram observados em um banco de dados do RDS em seu ambiente. AWS Uma tenthabilita malsucedida de login de endereços IP públicos pode indicar que o banco de dados do RDS em sua conta foi sujeito a uma tenthabilita de ataque de força bruta por um agente potencialmente malicioso.

Esses logins com falha foram identificados como anômalos pelo modelo de machine learning (ML) de detecção de anomalias do GuardDuty. O modelo de ML avalia todos os eventos de login do seu banco de dados Bancos de dados do Amazon Aurora compatíveis e identifica eventos anômalos associados às técnicas usadas pelos adversários. O modelo ML rastreia vários fatores da atividade de login do RDS, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e os detalhes específicos da conexão do banco de dados que foram usados. Para obter informações sobre as atividades de login do RDS que são potencialmente incomuns, consulteAnomalias baseadas na atividade de login do RDS.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, isso pode indicar que o banco de dados está exposto publicamente ou que há uma política de acesso excessivamente permissiva ao banco de dados. É recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigindo um banco de dados potencialmente comprometido com eventos de login falhados.

CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce

Um usuário fez login com sucesso em um banco de dados do RDS em sua conta a partir de um endereço IP público de forma anômala após um padrão consistente de tentativas incomuns de login malsucedidas.

Severidade padrão: alta

- Atributo: monitoramento de atividade de login do RDS

Essa descoberta informa que um login anômalo indichabilito de uma força bruta bem-sucedida foi observado em um banco de dados do RDS em seu ambiente. AWS Antes de um login bem-sucedido anômalo, foi observado um padrão consistente de tentativas incomuns de login malsucedidas. Isso indica que o usuário e a senha associados ao banco de dados do RDS em sua conta podem ter sido comprometidos e o banco de dados do RDS pode ter sido acessado por um agente potencialmente mal-intencionado.

Esse login bem-sucedido de força bruta foi identificado como anômalo pelo modelo de machine learning (ML) de detecção de anomalias do GuardDuty. O modelo de ML avalia todos os eventos de login do seu banco de dados Bancos de dados do Amazon Aurora compatíveis e identifica

eventos anômalos associados às técnicas usadas pelos adversários. O modelo ML rastreia vários fatores da atividade de login do RDS, como o usuário que fez a solicitação, o local de onde a solicitação foi feita e os detalhes específicos da conexão do banco de dados que foram usados. Para obter informações sobre as atividades de login do RDS que são potencialmente incomuns, consulteAnomalias baseadas na atividade de login do RDS.

Recomendações de correção:

Essa atividade indica que as credenciais do banco de dados podem ter sido expostas ou comprometidas. É recomendável alterar a senha do usuário do banco de dados associado e revisar os registros de auditoria disponíveis para a atividade realizada pelo usuário potencialmente comprometido. Um padrão consistente de tentativas incomuns de login malsucedidas indica que uma política de acesso excessivamente permissiva ao banco de dados ou o banco de dados também pode ter sido exposto publicamente. É recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigir um banco de dados potencialmente comprometido com eventos de login bem-sucedidos.

CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin

Um usuário fez login com sucesso em um banco de dados do RDS em sua conta a partir de um endereço IP malicioso conhecido.

Severidade padrão: alta

- Atributo: monitoramento de atividade de login do RDS

Essa descoberta informa que uma atividade bem-sucedida de login do RDS ocorreu a partir de um endereço IP associado a uma atividade maliciosa conhecida em seu AWS ambiente. Isso indica que o usuário e a senha associados ao banco de dados do RDS em sua conta podem ter sido comprometidos e o banco de dados do RDS pode ter sido acessado por um agente potencialmente mal-intencionado.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, isso pode indicar que as credenciais do usuário podem ter sido expostas ou comprometidas. É recomendável alterar a senha do usuário do banco de dados associado e revisar os registros de auditoria disponíveis para a

atividade realizada pelo usuário comprometido. Essa atividade também pode indicar que há uma política de acesso excessivamente permissiva ao banco de dados ou que o banco de dados está exposto publicamente. É recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigir um banco de dados potencialmente comprometido com eventos de login bem-sucedidos.

CredentialAccess:RDS/MaliciousIPCaller.FailedLogin

Um endereço IP associado a uma atividade maliciosa conhecida tentou, sem sucesso, fazer login em um banco de dados do RDS em sua conta.

Severidade padrão: média

- Atributo: monitoramento de atividade de login do RDS

Essa descoberta informa que um endereço IP associado a uma atividade maliciosa conhecida tentou fazer login em um banco de dados do RDS em seu AWS ambiente, mas não forneceu o nome de usuário ou a senha corretos. Isso indica que um agente potencialmente mal-intencionado pode estar tentando comprometer o banco de dados do RDS em sua conta.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, isso pode indicar que há uma política de acesso excessivamente permissiva ao banco de dados ou que o banco de dados está exposto publicamente. É recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigindo um banco de dados potencialmente comprometido com eventos de login falhados.

Discovery:RDS/MaliciousIPCaller

Um endereço IP associado a uma atividade maliciosa conhecida investigou um banco de dados do RDS em sua conta; nenhuma tenthabilita de autenticação foi feita.

Severidade padrão: média

- Atributo: monitoramento de atividade de login do RDS

Essa descoberta informa que um endereço IP associado a uma atividade maliciosa conhecida investigou um banco de dados do RDS em seu AWS ambiente, embora nenhuma tenthabilita de login tenha sido feita. Isso pode indicar que um agente potencialmente malicioso está tentando escanear uma infraestrutura acessível ao público.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, isso pode indicar que há uma política de acesso excessivamente permissiva ao banco de dados ou que o banco de dados está exposto publicamente. É recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigindo um banco de dados potencialmente comprometido com eventos de login falhados.

CredentialAccess:RDS/TorIPCaller.SuccessfulLogin

Um usuário fez login com sucesso em um banco de dados do RDS em sua conta a partir de um endereço IP do nó de saída do Tor.

Severidade padrão: alta

- Atributo: monitoramento de atividade de login do RDS

Essa descoberta informa que um usuário fez login com sucesso em um banco de dados do RDS em seu AWS ambiente, a partir de um endereço IP do nó de saída do Tor. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar um acesso não autorizado aos seus recursos do RDS com a intenção de ocultar a verdadeira identidade do usuário anônimo.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, isso pode indicar que as credenciais do usuário podem ter sido expostas ou comprometidas. É recomendável alterar a senha do usuário do banco de dados associado e revisar os registros de auditoria disponíveis para a atividade realizada pelo usuário comprometido. Essa atividade também pode indicar que há uma política de acesso excessivamente permissiva ao banco de dados ou que o banco de dados está

exposto publicamente. É recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigir um banco de dados potencialmente comprometido com eventos de login bem-sucedidos.

CredentialAccess:RDS/TorIPCaller.FailedLogin

Um endereço IP do Tor tentou fazer login sem sucesso em um banco de dados do RDS em sua conta.

Severidade padrão: média

- Atributo: monitoramento de atividade de login do RDS

Essa descoberta informa que um endereço IP do nó de saída do Tor tentou fazer login em um banco de dados do RDS em seu AWS ambiente, mas falhou em fornecer o nome de usuário ou a senha corretos. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar um acesso não autorizado aos seus recursos do RDS com a intenção de ocultar a verdadeira identidade do usuário anônimo.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, isso pode indicar que há uma política de acesso excessivamente permissiva ao banco de dados ou que o banco de dados está exposto publicamente. É recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigindo um banco de dados potencialmente comprometido com eventos de login falhados.

Discovery:RDS/TorIPCaller

Um endereço IP do nó de saída do Tor investigou um banco de dados RDS em sua conta, nenhuma tenthabilita de autenticação foi feita.

Severidade padrão: média

- Atributo: monitoramento de atividade de login do RDS

Essa descoberta informa que um endereço IP do nó de saída do Tor sondou um banco de dados RDS em seu AWS ambiente, embora nenhuma tenthabilita de login tenha sido feita. Isso pode indicar que um agente potencialmente malicioso está tentando escanear a infraestrutura acessível ao público. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar um acesso não autorizado aos recursos do RDS em sua conta com a intenção de ocultar a verdadeira identidade do invasor potencialmente nocivo.

Recomendações de correção:

Se essa atividade for inesperada para o banco de dados associado, isso pode indicar que há uma política de acesso excessivamente permissiva ao banco de dados ou que o banco de dados está exposto publicamente. É recomendável colocar o banco de dados em uma VPC privada e limitar as regras do grupo de segurança para permitir tráfego somente das fontes necessárias. Para obter mais informações, consulte Corrigindo um banco de dados potencialmente comprometido com eventos de login falhados.

Tipos de descoberta de monitoramento de tempo de execução

A Amazon GuardDuty gera as seguintes descobertas do Runtime Monitoring para indicar possíveis ameaças com base no comportamento em nível de sistema operacional dos hosts e contêineres do Amazon EC2 em seus clusters do Amazon EKS, cargas de trabalho do Fargate e do Amazon ECS e instâncias do Amazon EC2.

> **Note**
>
> Os tipos de descoberta do Monitoramento de runtime são baseados nos registros de runtime coletados dos hosts. Os registros contêm campos, como caminhos de arquivos, que podem ser controlados por um agente mal-intencionado. Esses campos também estão incluídos nas GuardDuty descobertas para fornecer contexto de tempo de execução. Ao processar as descobertas do Runtime Monitoring fora do GuardDuty console, você deve limpar os campos de busca. Por exemplo, é possível codificar em HTML os campos de busca ao exibi-los em uma página da Web.

Tópicos

- CryptoCurrency:Runtime/BitcoinTool.B

- Backdoor:Runtime/C&CActivity.B
- UnauthorizedAccess:Runtime/TorRelay
- UnauthorizedAccess:Runtime/TorClient
- Trojan:Runtime/BlackholeTraffic
- Trojan:Runtime/DropPoint
- CryptoCurrency:Runtime/BitcoinTool.B!DNS
- Backdoor:Runtime/C&CActivity.B!DNS
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS
- Impact:Runtime/AbusedDomainRequest.Reputation
- Impact:Runtime/BitcoinDomainRequest.Reputation
- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- UnauthorizedAccess:Runtime/MetadataDNSRebind
- Execution:Runtime/NewBinaryExecuted
- PrivilegeEscalation:Runtime/DockerSocketAccessed
- PrivilegeEscalation:Runtime/RuncContainerEscape
- PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified
- DefenseEvasion:Runtime/ProcessInjection.Proc
- DefenseEvasion:Runtime/ProcessInjection.Ptrace
- DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite
- Execution:Runtime/ReverseShell
- DefenseEvasion:Runtime/FilelessExecution
- Impact:Runtime/CryptoMinerExecuted
- Execution:Runtime/NewLibraryLoaded
- PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

- PrivilegeEscalation:Runtime/UserfaultfdUsage
- Execution:Runtime/SuspiciousTool
- Execution:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/SuspiciousCommand
- DefenseEvasion:Runtime/PtraceAntiDebugging
- Execution:Runtime/MaliciousFileExecuted

CryptoCurrency:Runtime/BitcoinTool.B

Uma instância do Amazon EC2 ou um contêiner está consultando um endereço IP associado à atividade relacionada à criptomoeda.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que a instância do EC2 listada ou um contêiner em seu ambiente da AWS está consultando um endereço IP associado a uma atividade relacionada a criptomoedas. Os agentes de ameaças podem tentar assumir o controle dos recursos computacionais para redirecioná-los de maneira mal-intencionada para a mineração não autorizada de criptomoedas.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se você usar essa instância do EC2 ou um contêiner para minerar ou gerenciar criptomoeda, ou se essa instância ou contêiner estiverem envolvidos de outra forma na atividade de blockchain, a descoberta CryptoCurrency:Runtime/BitcoinTool.B poderia representar uma atividade esperada para o ambiente. Se esse for o caso em seu AWS ambiente, recomendamos que você configure uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `CryptoCurrency:Runtime/BitcoinTool.B`. O segundo critério de filtro deve ser o ID da instância ou o ID da imagem do contêiner envolvido na atividade relacionada à criptomoeda ou blockchain. Para obter mais informações, consulte Regras de supressão.

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Backdoor:Runtime/C&CActivity.B

Uma instância do Amazon EC2 ou um contêiner está consultando um nome de domínio associado a um servidor de comando e controle conhecido.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que existe uma instância do EC2 ou um contêiner no seu ambiente da AWS que está consultando um IP associado a um servidor conhecido de comando e controle (C&C). A instância ou o contêiner listado podem estar potencialmente comprometidos. Os servidores de comando e controle são computadores que enviam comandos para membros de um botnet.

Um botnet é uma coleção de dispositivos conectados à Internet (que podem incluir PCs, servidores, dispositivos móveis e dispositivos de Internet das Coisas) infectados e controlados por um tipo comum de malware. Os botnets são frequentemente usados para distribuir malwares e coletar informações inapropriadas, como números de cartão de crédito. Dependendo da finalidade e da estrutura do botnet, o servidor C&C também pode emitir comandos para iniciar um ataque de negação distribuída de serviço DDoS.

> **Note**
>
> Se o IP consultado estiver relacionado ao log4j, os campos da descoberta associada incluirão os seguintes valores:
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

UnauthorizedAccess:Runtime/TorRelay

Sua instância do Amazon EC2 ou um contêiner está fazendo conexões com uma rede Tor como uma retransmissão Tor.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que uma instância do EC2 ou um contêiner em seu AWS ambiente está fazendo conexões com uma rede Tor de uma maneira que sugere que ela está agindo como um retransmissor Tor. Tor é um software para permitir a comunicação anônima. Retransmissões Tor aumentam o anonimato da comunicação encaminhando o tráfego possivelmente ilícito do cliente de uma retransmissão Tor para outra.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

UnauthorizedAccess:Runtime/TorClient

Sua instância do Amazon EC2 ou um contêiner está fazendo conexões com um Tor Guard ou um nó de autoridade.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que uma instância do EC2 ou um contêiner em seu AWS ambiente está fazendo conexões com um Tor Guard ou um nó de Autoridade. Tor é um software para permitir a comunicação anônima. Tor Guards ou nós de autoridade atuam como gateways iniciais em uma rede do Tor. Esse tráfego pode indicar que a instância do EC2 ou o contêiner foi possivelmente comprometido e está agindo com um cliente em uma rede Tor. Essa descoberta pode indicar acesso não autorizado aos seus AWS recursos com a intenção de ocultar a verdadeira identidade do atacante.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Trojan:Runtime/BlackholeTraffic

Uma instância do Amazon EC2 ou um contêiner está tentando se comunicar com um endereço IP de um host remoto que é um buraco negro conhecido.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que a instância do EC2 listada ou um contêiner em seu AWS ambiente pode estar comprometido porque está tentando se comunicar com o endereço IP de um buraco negro (ou sumidouro). Os buracos negros são locais na rede onde o tráfego de entrada ou de saída é descartado silenciosamente sem informar a fonte de que os dados não atingiram o destinatário pretendido. Um endereço IP de buraco negro especifica uma máquina host que não está sendo executada ou um endereço para o qual nenhum host foi atribuído.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Trojan:Runtime/DropPoint

Uma instância do Amazon EC2 ou um contêiner está tentando se comunicar com um endereço IP de um host remoto que é conhecido por manter credenciais e outros dados roubados capturados por malware.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que uma instância do EC2 ou um contêiner em seu AWS ambiente está tentando se comunicar com um endereço IP de um host remoto que é conhecido por conter credenciais e outros dados roubados capturados por malware.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

CryptoCurrency:Runtime/BitcoinTool.B!DNS

Uma instância do Amazon EC2 ou um contêiner está consultando um nome de domínio associado a uma atividade de criptomoeda.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que a instância do EC2 listada ou um contêiner em seu ambiente da AWS está consultando um nome de domínio associado ao Bitcoin ou a outras atividades relacionadas a criptomoedas. Os agentes de ameaças podem tentar assumir o controle dos recursos computacionais a fim de redirecioná-los de maneira mal-intencionada para a mineração não autorizada de criptomoedas.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se você usar essa instância do EC2 ou contêiner para minerar ou gerenciar criptomoeda, ou se essa instância ou contêiner estiverem envolvidos de outra forma na atividade de blockchain, a descoberta CryptoCurrency:Runtime/BitcoinTool.B!DNS poderia ser uma atividade esperada para o ambiente. Se esse for o caso em seu AWS ambiente, recomendamos que você configure uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `CryptoCurrency:Runtime/BitcoinTool.B!DNS`. O segundo critério de filtro deve ser o ID de instância da instância ou o ID da imagem do contêiner do contêiner envolvido na atividade de criptomoedas ou blockchain. Para obter mais informações, consulte Regras de supressão.

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Backdoor:Runtime/C&CActivity.B!DNS

A instância do Amazon EC2 ou um contêiner está consultando um nome de domínio associado a um servidor de comando e controle conhecido.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que a instância do EC2 ou o contêiner listado em seu ambiente da AWS está consultando um nome de domínio associado a um servidor de comando e controle (C&C)

conhecido. A instância EC2 listada ou o contêiner podem estar comprometidos. Os servidores de comando e controle são computadores que enviam comandos para membros de um botnet.

Um botnet é uma coleção de dispositivos conectados à Internet, que podem incluir PCs, servidores, dispositivos móveis e dispositivos de Internet das Coisas, infectados e controlados por um tipo comum de malware. Os botnets são frequentemente usados para distribuir malwares e coletar informações inapropriadas, como números de cartão de crédito. Dependendo da finalidade e da estrutura do botnet, o servidor C&C também pode emitir comandos para iniciar um ataque de negação distribuída de serviço DDoS.

> **Note**
>
> Se o nome de domínio consultado estiver relacionado ao log4j, os campos da descoberta associada incluirão os seguintes valores:
>
> - `service.additionalInfo.threatListName = Amazon`
> - `service.additionalInfo.threatName = Log4j Related`

> **Note**
>
> Para testar como GuardDuty gera esse tipo de descoberta, você pode fazer uma solicitação de DNS da sua instância (usando `dig` para Linux ou `nslookup` Windows) em um domínio `guarddutyc2activityb.com` de teste.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Trojan:Runtime/BlackholeTraffic!DNS

Uma instância do Amazon EC2 ou um contêiner está consultando um nome de domínio que está sendo redirecionado para o endereço IP de um buraco negro.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que a instância do EC2 listada ou o contêiner em seu ambiente da AWS pode estar comprometido porque está consultando um nome de domínio que está sendo redirecionado para um endereço IP de buraco negro. Os buracos negros são locais na rede onde o tráfego de entrada ou de saída é descartado silenciosamente sem informar a fonte de que os dados não atingiram o destinatário pretendido.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Trojan:Runtime/DropPoint!DNS

Uma instância do Amazon EC2 ou um contêiner está consultando um nome de domínio de um host remoto que é conhecido por manter credenciais e outros dados roubados capturados por malware.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que uma instância do EC2 ou um contêiner em seu AWS ambiente está consultando o nome de domínio de um host remoto que é conhecido por conter credenciais e outros dados roubados capturados por malware.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Trojan:Runtime/DGADomainRequest.C!DNS

Uma instância do Amazon EC2 ou um contêiner está consultando domínios gerados por algoritmos. Esses domínios são comumente usados por malware e podem ser um indicativo de uma instância do EC2 ou um contêiner comprometido.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que a instância do EC2 ou o contêiner listado no seu ambiente da AWS está tentando consultar domínios do algoritmo de geração de domínio (DGA). Seu recurso pode ter sido comprometido.

Os DGAs são usados para gerar uma grande quantidade de nomes de domínio periodicamente que podem ser usados como pontos de encontro com seus servidores de comando e controle (C&C). Os servidores de comando e controle são computadores que emitem comandos para membros de um botnet, ou seja, uma coleção de dispositivos conectados à Internet infectados e controlados por um tipo comum de malware. O grande número de pontos de encontro potenciais dificulta o encerramento efetivo dos botnets, uma vez que os computadores infectados tentam entrar em contato com alguns desses nomes de domínio todos os dias para receber atualizações ou comandos.

> **Note**
>
> Essa descoberta é baseada em domínios DGA conhecidos de feeds de inteligência de GuardDuty ameaças.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Trojan:Runtime/DriveBySourceTraffic!DNS

Uma instância do Amazon EC2 ou um contêiner está consultando um nome de domínio de um host remoto que é uma fonte conhecida de ataques Drive-by download.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que a instância do EC2 listada ou o contêiner em seu ambiente da AWS pode estar comprometido porque está consultando um nome de domínio de um host remoto que é uma fonte conhecida de ataques de download drive-by. Estes são downloads indesejados de software de computador da Internet que podem acionar uma instalação automática de vírus, spyware ou malware.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Trojan:Runtime/PhishingDomainRequest!DNS

Uma instância do Amazon EC2 ou um contêiner está consultando domínios envolvidos em ataques de phishing.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que existe uma instância do EC2 ou um contêiner no seu ambiente da AWS que está tentando consultar um domínio envolvido em ataques de phishing. Domínios de phishing são configuradas por alguém se passando por uma instituição legítima para induzir indivíduos a

fornecerem dados confidenciais, como informações de identificação pessoal, dados bancários e de cartão de crédito, e senhas. Sua instância do EC2 ou o contêiner pode estar tentando recuperar dados confidenciais armazenados em um site de phishing ou pode estar tentando configurar um site de phishing. Sua instância do EC2 ou o contêiner pode estar comprometido.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Impact:Runtime/AbusedDomainRequest.Reputation

Uma instância do Amazon EC2 ou um contêiner está consultando um nome de domínio de baixa reputação que está associado a domínios conhecidos por abuso.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que a instância do EC2 listada ou o contêiner em seu ambiente da AWS está consultando um nome de domínio de baixa reputação associado a domínios ou endereços IP de abuso conhecidos. Exemplos de domínios abusados são nomes de domínio de nível superior (TLDs) e nomes de domínio de segundo nível (2LDs) que fornecem registros gratuitos de subdomínios, bem como provedores de DNS dinâmicos. Os agentes de ameaças tendem a usar esses serviços para registrar domínios gratuitamente ou a baixo custo. Os domínios de baixa reputação nessa categoria também podem ser domínios expirados que se resolvem para o endereço IP estacionário de um registrador e, portanto, podem não estar mais ativas. Um IP de estacionamento é onde um registrador direciona o tráfego para domínios que não foram vinculados a nenhum serviço. A instância listada do Amazon EC2 ou o contêiner podem estar comprometidos, pois os agentes de ameaças geralmente usam esses registradores ou serviços para C&C e distribuição de malware.

Os domínios de baixa reputação são baseados em um modelo de pontuação de reputação. Esse modelo avalia e classifica as características de um domínio para determinar sua probabilidade de ser mal-intencionado.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Impact:Runtime/BitcoinDomainRequest.Reputation

Uma instância do Amazon EC2 ou um contêiner está consultando um nome de domínio associado à atividade relacionada à criptomoeda.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa a você que uma instância do EC2 ou contêiner em seu ambiente da AWS está consultando um nome de domínio de baixa reputação associado à Bitcoin ou a atividades relacionadas a outras criptomoedas. Os agentes de ameaças podem tentar assumir o controle dos recursos computacionais para redirecioná-los de maneira mal-intencionada para a mineração não autorizada de criptomoedas.

Os domínios de baixa reputação são baseados em um modelo de pontuação de reputação. Esse modelo avalia e classifica as características de um domínio para determinar sua probabilidade de ser mal-intencionado.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se você usar essa instância do EC2 ou contêiner para minerar ou gerenciar criptomoeda ou se essa instância estiver envolvida de outra forma na atividade de blockchain, essa descoberta poderia representar a atividade esperada para o ambiente. Se esse for o caso em seu AWS ambiente, recomendamos que você configure uma regra de supressão para essa descoberta. A regra de

supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `Impact:Runtime/BitcoinDomainRequest.Reputation`. O segundo critério de filtro deve ser o ID da instância ou o ID da imagem do contêiner envolvido em atividades relacionadas à criptomoeda ou blockchain. Para obter mais informações, consulte Regras de supressão.

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Impact:Runtime/MaliciousDomainRequest.Reputation

Uma instância do Amazon EC2 ou um contêiner está consultando um domínio de baixa reputação associado a domínios mal-intencionados conhecidos.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que a instância do EC2 listada ou o contêiner em seu ambiente da AWS está consultando um nome de domínio de baixa reputação associado a domínios ou endereços IP mal-intencionados conhecidos. Por exemplo, os domínios podem estar associados a um endereço IP sumidouro conhecido. Domínios sinkholed são domínios que antes eram controlados por um agente de ameaças, e as solicitações feitas a eles podem indicar que a instância está comprometida. Esses domínios também podem estar correlacionados com campanhas mal-intencionadas conhecidas ou algoritmos de geração de domínio.

Os domínios de baixa reputação são baseados em um modelo de pontuação de reputação. Esse modelo avalia e classifica as características de um domínio para determinar sua probabilidade de ser mal-intencionado.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Impact:Runtime/SuspiciousDomainRequest.Reputation

Uma instância do Amazon EC2 ou um contêiner está consultando um nome de domínio de baixa reputação que é suspeito por natureza devido à sua idade ou baixa popularidade.

Gravidade padrão: baixa

- Atributo: Monitoramento de runtime

Essa descoberta informa que a instância EC2 listada ou o contêiner em seu ambiente da AWS está consultando um nome de domínio de baixa reputação que é suspeito de ser mal-intencionado. Percebi características desse domínio que eram consistentes com domínios mal-intencionados observados anteriormente, no entanto, nosso modelo de reputação não conseguiu relacioná-lo definitivamente a uma ameaça conhecida. Esses domínios geralmente são observados recentemente ou recebem uma quantidade baixa de tráfego.

Os domínios de baixa reputação são baseados em um modelo de pontuação de reputação. Esse modelo avalia e classifica as características de um domínio para determinar sua probabilidade de ser mal-intencionado.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

UnauthorizedAccess:Runtime/MetadataDNSRebind

Uma instância do Amazon EC2 ou um contêiner está executando pesquisas de DNS que são resolvidas como o serviço de metadados da instância.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

> **Note**
>
> Atualmente, esse tipo de descoberta só é suportado pela arquitetura AMD64.

Essa descoberta informa que uma instância do EC2 ou um contêiner em seu AWS ambiente está consultando um domínio que resolve para o endereço IP dos metadados do EC2 (169.254.169.254). Uma consulta ao DNS desse tipo pode indicar que a instância é alvo de uma técnica de revinculação de DNS. Essa técnica pode ser usada para obter metadados de uma instância do EC2, incluindo as credenciais do IAM associadas à instância.

A revinculação de DNS envolve enganar um aplicativo em execução na instância do EC2 para carregar dados de retorno de um URL, onde o nome de domínio no URL é resolvido como o endereço IP de metadados do EC2 (`169.254.169.254`). Isso faz com que o aplicativo acesse metadados do EC2 e possivelmente os disponibilize para o invasor.

É possível acessar metadados do EC2 usando a revinculação de DNS somente se a instância do EC2 estiver executando um aplicativo vulnerável que permita a injeção de URLs ou se um usuário humano acessar a URL em um navegador da web em execução na instância do EC2.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Em resposta a essa descoberta, você deve avaliar se há um aplicativo vulnerável em execução na instância do EC2 ou no contêiner, ou se um usuário humano usou um navegador para acessar o domínio identificado na descoberta. Se a causa raiz for um aplicativo vulnerável, você deverá corrigir a vulnerabilidade. Se for devido à navegação de um usuário no domínio identificado, bloqueie o domínio ou impeça que os usuários o acessem. Se você determinar que essa descoberta estava relacionada a qualquer um dos casos acima, deverá revogar a sessão associada à instância do EC2.

Alguns AWS clientes mapeiam intencionalmente o endereço IP dos metadados para um nome de domínio em seus servidores DNS autorizados. Se esse for o caso em seu ambiente da , recomendamos configurar uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `UnauthorizedAccess:Runtime/MetaDataDNSRebind`. O segundo critério de filtro deve ser o domínio de solicitação de DNS ou o ID da imagem do contêiner. O valor do

Domínio da solicitação DNS deve corresponder ao domínio que você mapeou para o endereço IP de metadados (`169.254.169.254`). Para obter informações sobre a criação de regras de supressão, consulte Regras de supressão.

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Execution:Runtime/NewBinaryExecuted

Um arquivo binário recém-criado ou modificado recentemente em um contêiner foi executado.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que um arquivo binário recém-criado ou modificado recentemente em um contêiner foi executado. É a melhor prática manter os contêineres imutáveis em runtime, e arquivos binários, scripts ou bibliotecas não devem ser criados ou modificados durante a vida útil do contêiner. Esse comportamento indica que um agente mal-intencionado que obteve acesso ao contêiner, baixou e executou malware ou outro software como parte do possível comprometimento. Embora esse tipo de atividade possa ser uma indicação de comprometimento, também é um padrão de uso comum. Portanto, GuardDuty usa mecanismos para identificar instâncias suspeitas dessa atividade e gera esse tipo de descoberta somente para instâncias suspeitas.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

PrivilegeEscalation:Runtime/DockerSocketAccessed

Um processo dentro de um contêiner está se comunicando com o daemon do Docker usando o soquete Docker.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

O soquete Docker é um soquete de domínio Unix que o daemon do Docker (`dockerd`) usa para se comunicar com seus clientes. Um cliente pode realizar várias ações, como criar contêineres comunicando-se com o daemon do Docker por meio do soquete do Docker. É suspeito que um processo de contêiner acesse o soquete do Docker. Um processo de contêiner pode escapar do contêiner e obter acesso no nível do host comunicando-se com o soquete do Docker e criando um contêiner privilegiado.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

PrivilegeEscalation:Runtime/RuncContainerEscape

Foi detectada uma tentativa de obter acesso ao host de um contêiner.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que o arquivo binário runC do host foi potencialmente sobrescrito. O runC é o runtime de contêiner de baixo nível que tempos de execução de contêiner de alto nível, como Docker e Containerd, usam para gerar e executar contêineres. O runC é sempre executado com privilégios de root porque precisa executar uma tarefa de baixo nível de criação de um contêiner. Uma vulnerabilidade [1] bem conhecida no passado permitia que contêineres maliciosos substituíssem o arquivo binário rUNC do host e obtivessem acesso no nível raiz ao host quando o binário rUNC modificado era executado.

Essa descoberta também pode indicar que um agente mal-intencionado potencialmente executou um comando em um dos dois tipos de contêineres a seguir:

- Um novo contêiner com uma imagem controlada pelo atacante.
- Um contêiner existente que antes era acessível ao invasor com permissões de gravação.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

- 1. Detalhe do CVE-2019-5736

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified

Um escape de contêiner por meio do runC foi detectado em um cluster do Amazon EKS.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que foi detectada uma tentativa de modificar um arquivo do agente de liberação do grupo de controle (cgroup). O Linux usa grupos de controle (cgroups) para limitar, contabilizar e isolar o uso de recursos de uma coleção de processos. Cada cgroup tem um arquivo de agente de lançamento (`release_agent`), um script que o Linux executa quando qualquer processo dentro do cgroup é encerrado. O arquivo do agente de liberação é sempre executado no nível do host. Um agente de ameaça dentro de um contêiner pode escapar para o host escrevendo comandos arbitrários no arquivo do agente de lançamento que pertence a um cgroup. Quando um processo dentro desse cgroup termina, os comandos escritos pelo ator são executados.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

DefenseEvasion:Runtime/ProcessInjection.Proc

Uma injeção de processo usando o sistema de arquivos proc foi detectada em um contêiner ou em uma instância do Amazon EC2.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

A injeção de processos é uma técnica que os agentes de ameaças usam para injetar código nos processos para evitar as defesas e potencialmente elevar os privilégios. O sistema de arquivos proc (procfs) é um sistema de arquivos especial no Linux que apresenta a memória virtual do processo como um arquivo. O caminho desse arquivo é `/proc/PID/mem`, onde `PID` é o ID exclusivo do processo. Um agente de ameaça pode gravar nesse arquivo para injetar código no processo. Essa descoberta identifica possíveis tentativas de gravação nesse arquivo.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu tipo de recurso pode ter sido comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

DefenseEvasion:Runtime/ProcessInjection.Ptrace

Uma injeção de processo usando a chamada do sistema ptrace foi detectada em um contêiner ou em uma instância do Amazon EC2.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

A injeção de processos é uma técnica que os agentes de ameaças usam para injetar código nos processos para evitar as defesas e potencialmente elevar os privilégios. Um processo pode usar a chamada do sistema ptrace para injetar código em outro processo. Essa descoberta identifica uma possível tentativa de injetar código em um processo usando a chamada de sistema ptrace.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu tipo de recurso pode ter sido comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite

Uma injeção de processo por meio de uma gravação direta na memória virtual foi detectada em um contêiner ou em uma instância do Amazon EC2.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

A injeção de processos é uma técnica que os agentes de ameaças usam para injetar código nos processos para evitar as defesas e potencialmente elevar os privilégios. Um processo pode usar uma chamada de sistema, por exemplo, `process_vm_writev` para injetar código diretamente na memória virtual de outro processo. Essa descoberta identifica uma possível tentativa de injetar código em um processo usando uma chamada de sistema para gravação na memória virtual do processo.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu tipo de recurso pode ter sido comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Execution:Runtime/ReverseShell

Um processo em um contêiner ou instância do Amazon EC2 criou um shell reverso.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Um shell reverso é uma sessão de shell criada em uma conexão que é iniciada do host de destino para o host do ator. Isso é o oposto de um shell normal iniciado do hospedeiro do agente para o hospedeiro do destino. Os agentes da ameaça criam um shell reverso para executar comandos no alvo depois de obter acesso inicial ao alvo. Essa descoberta identifica uma possível tentativa de criar um shell reverso.

Recomendações de correção:

Se essa atividade for inesperada, seu tipo de recurso pode ter sido comprometido.

DefenseEvasion:Runtime/FilelessExecution

Um processo em um contêiner ou instância do Amazon EC2 está executando código a partir da memória.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa quando um processo é executado usando um arquivo executável na memória no disco. Essa é uma técnica comum de evasão de defesa que evita gravar o executável mal-intencionado no disco para evitar a detecção baseada na verificação do sistema de arquivos. Embora essa técnica seja usada por malware, ela também tem alguns casos de uso legítimos. Um dos exemplos é um compilador just-in-time (JIT) que grava código compilado na memória e o executa a partir da memória.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Impact:Runtime/CryptoMinerExecuted

Um contêiner ou uma instância do Amazon EC2 está executando um arquivo binário associado a uma atividade de mineração de criptomoedas.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que um contêiner ou uma instância do EC2 em seu AWS ambiente está executando um arquivo binário associado a uma atividade de mineração de criptomoedas. Os agentes de ameaças podem tentar assumir o controle dos recursos computacionais para redirecioná-los de maneira mal-intencionada para a mineração não autorizada de criptomoedas.

O agente de runtime monitora eventos de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso no painel de descobertas no GuardDuty console.

Recomendações de correção:

O agente de runtime monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console e vejaCorreção das descobertas do Runtime Monitoring.

Execution:Runtime/NewLibraryLoaded

Uma biblioteca recém-criada ou modificada recentemente foi carregada por um processo dentro de um contêiner.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Essa descoberta informa que uma biblioteca foi criada ou modificada dentro de um contêiner durante o runtime e carregada por um processo executado dentro do contêiner. A melhor prática é manter os contêineres imutáveis no runtime e não criar ou modificar os arquivos binários, scripts ou bibliotecas durante a vida útil do contêiner. O carregamento de uma biblioteca recém-criada ou modificada em um contêiner pode indicar atividade suspeita. Esse comportamento indica que um agente mal-intencionado potencialmente obteve acesso ao contêiner, baixou e executou malware ou outro software como parte do possível comprometimento. Embora esse tipo de atividade possa ser uma indicação de comprometimento, também é um padrão de uso comum. Portanto, GuardDuty usa mecanismos para identificar instâncias suspeitas dessa atividade e gera esse tipo de descoberta somente para instâncias suspeitas.

O agente de runtime monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

PrivilegeEscalation:Runtime/ContainerMountsHostDirectory

Um processo dentro de um contêiner montou um sistema de arquivos hospedeiro em runtime.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Várias técnicas de escape de contêiner envolvem a montagem de um sistema de arquivos hospedeiro dentro de um contêiner em runtime. Essa descoberta informa que um processo dentro de um contêiner potencialmente tentou montar um sistema de arquivos do host, o que pode indicar uma tentativa de escapar para o host.

O agente de runtime monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

PrivilegeEscalation:Runtime/UserfaultfdUsage

Um processo usou chamadas de sistema **`userfaultfd`** para lidar com falhas de página no espaço do usuário.

Gravidade padrão: média

- Atributo: Monitoramento de runtime

Normalmente, as falhas de página são tratadas pelo kernel no espaço do kernel. No entanto, a chamada de sistema `userfaultfd` permite que um processo manipule falhas de página em um sistema de arquivos no espaço do usuário. Esse é um recurso útil que permite a implementação de sistemas de arquivos no espaço do usuário. Por outro lado, ele também pode ser usado por um processo potencialmente mal-intencionado para interromper o kernel do espaço do usuário. Interromper o kernel usando a chamada de sistema `userfaultfd` é uma técnica de exploração comum para estender as janelas de corrida durante a exploração das condições de corrida do kernel. O uso de `userfaultfd` pode indicar atividade suspeita na instância do Amazon Elastic Compute Cloud (Amazon EC2).

O agente de runtime monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Execution:Runtime/SuspiciousTool

Um contêiner ou uma instância do Amazon EC2 está executando um arquivo binário ou script que é frequentemente usado em cenários de segurança ofensivos, como testes de engajamento.

Gravidade padrão: variável

A gravidade dessa descoberta pode ser alta ou baixa, dependendo se a ferramenta suspeita detectada é considerada de uso duplo ou se é exclusivamente para uso ofensivo.

- Atributo: Monitoramento de runtime

Essa descoberta informa que uma ferramenta suspeita foi executada em uma instância ou contêiner do EC2 em seu AWS ambiente. Isso inclui ferramentas usadas em projetos de pentesting, também conhecidas como ferramentas de backdoor, scanners de rede e detectores de rede. Todas essas ferramentas podem ser usadas em contextos benignos, mas também são frequentemente usadas por agentes de ameaças com intenções maliciosas. A observação de ferramentas de segurança ofensivas pode indicar que a instância ou o contêiner EC2 associado foi comprometido.

GuardDuty examina a atividade e o contexto de tempo de execução relacionados para gerar essa descoberta somente quando a atividade e o contexto associados forem potencialmente suspeitos.

O agente de runtime monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Execution:Runtime/SuspiciousCommand

Um comando suspeito foi executado em uma instância do Amazon EC2 ou em um contêiner que indica um comprometimento.

Gravidade padrão: variável

Dependendo do impacto do padrão malicioso observado, a gravidade desse tipo de descoberta pode ser baixa, média ou alta.

- Atributo: Monitoramento de runtime

Essa descoberta informa que um comando suspeito foi executado e indica que uma instância do Amazon EC2 ou um contêiner em AWS seu ambiente foi comprometido. Isso pode significar que um

arquivo foi baixado de uma fonte suspeita e depois executado, ou que um processo em execução exibe um padrão malicioso conhecido em sua linha de comando. Isso indica ainda que o malware está sendo executado no sistema.

GuardDuty examina a atividade e o contexto de tempo de execução relacionados para gerar essa descoberta somente quando a atividade e o contexto associados forem potencialmente suspeitos.

O agente de runtime monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

DefenseEvasion:Runtime/SuspiciousCommand

Um comando executado na instância listada do Amazon EC2 ou em um contêiner tenta modificar ou desativar um mecanismo de defesa do Linux, como firewall ou serviços essenciais do sistema.

Gravidade padrão: variável

Dependendo de qual mecanismo de defesa foi modificado ou desativado, a gravidade desse tipo de descoberta pode ser alta, média ou baixa.

- Atributo: Monitoramento de runtime

Essa descoberta informa que um comando que tenta ocultar um ataque dos serviços de segurança do sistema local foi executado. Isso inclui ações como desabilitar o firewall Unix, modificar tabelas IP locais, remover crontab entradas, desabilitar um serviço local ou assumir a função. `LDPreload` Qualquer modificação é altamente suspeita e um potencial indicador de comprometimento. Portanto, esses mecanismos detectam ou evitam maiores comprometimentos do sistema.

GuardDuty examina a atividade e o contexto de tempo de execução relacionados para gerar essa descoberta somente quando a atividade e o contexto associados forem potencialmente suspeitos.

O agente de runtime monitora eventos de vários recursos. Para identificar o recurso potencialmente comprometido, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

DefenseEvasion:Runtime/PtraceAntiDebugging

Um processo em um contêiner ou instância do Amazon EC2 executou uma medida anti-depuração usando a chamada do sistema ptrace.

Gravidade padrão: baixa

- Atributo: Monitoramento de runtime

Essa descoberta mostra que um processo em execução em uma instância do Amazon EC2 ou em um contêiner em seu AWS ambiente usou a chamada do sistema ptrace com a opção. `PTRACE_TRACEME` Essa atividade faria com que um depurador conectado se separasse do processo em execução. Se nenhum depurador estiver conectado, ele não terá efeito. No entanto, a atividade por si só levanta suspeitas. Isso pode indicar que o malware está sendo executado no sistema. O malware frequentemente usa técnicas de antidepuração para evitar a análise, e essas técnicas podem ser detectadas em tempo de execução.

GuardDuty examina a atividade e o contexto de tempo de execução relacionados para gerar essa descoberta somente quando a atividade e o contexto associados forem potencialmente suspeitos.

O agente de runtime monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

Execution:Runtime/MaliciousFileExecuted

Um arquivo executável malicioso conhecido foi executado em uma instância do Amazon EC2 ou em um contêiner.

Gravidade padrão: alta

- Atributo: Monitoramento de runtime

Essa descoberta informa que um executável malicioso conhecido foi executado na instância do Amazon EC2 ou em um contêiner em seu ambiente. AWS Esse é um forte indicador de que a instância ou o contêiner foram potencialmente comprometidos e que o malware foi executado.

O malware frequentemente usa técnicas de antidepuração para evitar a análise, e essas técnicas podem ser detectadas em tempo de execução.

GuardDuty examina a atividade e o contexto de tempo de execução relacionados para gerar essa descoberta somente quando a atividade e o contexto associados forem potencialmente suspeitos.

O agente de runtime monitora eventos de vários recursos. Para identificar o recurso afetado, veja o tipo de recurso nos detalhes das descobertas no GuardDuty console.

Recomendações de correção:

Se essa atividade for inesperada, seu recurso pode estar comprometido. Para ter mais informações, consulte Correção das descobertas do Runtime Monitoring.

GuardDuty Tipos de descoberta do S3

As descobertas a seguir são específicas dos recursos do Amazon S3 e terão um tipo de recurso de **`S3Bucket`** se a fonte de dados for eventos de CloudTrail dados do S3 ou **`AccessKey`** se a fonte de dados for CloudTrail eventos de gerenciamento. A gravidade e os detalhes das descobertas serão diferentes com base no tipo de descoberta e na permissão associada ao bucket.

As descobertas listadas aqui incluem as fontes de dados e os modelos usados para gerar esse tipo de descoberta. Para obter mais informações sobre modelos e fontes de dados, consulte Fontes de dados fundamentais.

> **Important**
>
> As descobertas com uma fonte de dados de eventos de CloudTrail dados para o S3 só são geradas se você tiver a proteção do S3 ativada para. GuardDuty A proteção do S3 está habilitada por padrão em todas as contas criadas após 31 de julho de 2020. Para obter informações sobre como habilitar ou desabilitar a proteção do S3, consulte Proteção do Amazon S3 na Amazon GuardDuty.

Para todos os `S3Bucket` tipos de descobertas, é recomendável que você examine as permissões no bucket em questão e as permissões de qualquer usuário envolvido na descoberta. Se a atividade for inesperada, consulte as recomendações de remediação detalhadas emCorrigindo um bucket S3 potencialmente comprometido.

Tópicos

- Discovery:S3/AnomalousBehavior
- Discovery:S3/MaliciousIPCaller
- Discovery:S3/MaliciousIPCaller.Custom
- Discovery:S3/TorIPCaller
- Exfiltration:S3/AnomalousBehavior
- Exfiltration:S3/MaliciousIPCaller
- Impact:S3/AnomalousBehavior.Delete
- Impact:S3/AnomalousBehavior.Permission
- Impact:S3/AnomalousBehavior.Write
- Impact:S3/MaliciousIPCaller
- PenTest:S3/KaliLinux
- PenTest:S3/ParrotLinux
- PenTest:S3/PentooLinux
- Policy:S3/AccountBlockPublicAccessDisabled
- Policy:S3/BucketAnonymousAccessGranted
- Policy:S3/BucketBlockPublicAccessDisabled
- Policy:S3/BucketPublicAccessGranted
- Stealth:S3/ServerAccessLoggingDisabled
- UnauthorizedAccess:S3/MaliciousIPCaller.Custom
- UnauthorizedAccess:S3/TorIPCaller

Discovery:S3/AnomalousBehavior

Uma API comumente usada para descobrir objetos do S3 foi invocada de forma anômala.

Gravidade padrão: baixa

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma entidade do IAM invocou uma API do S3 para descobrir buckets do S3 em seu ambiente, como `ListObjects`. Esse tipo de atividade está associado ao estágio de descoberta de um ataque, no qual um invasor coleta informações para determinar se seu AWS ambiente é suscetível a um ataque mais amplo. Essa atividade é suspeita porque a entidade do IAM invocou a API de uma forma incomum. Por exemplo, uma entidade do IAM sem histórico anterior invoca uma API do S3, ou uma entidade do IAM invoca uma API do S3 de um local incomum.

Essa API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. Ele rastreia vários fatores das solicitações de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, a API específica solicitada, o bucket solicitado e o número de chamadas de API feitas. Para obter mais informações sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação, consulte Como encontrar detalhes.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Discovery:S3/MaliciousIPCaller

Uma API do S3 comumente usada para descobrir recursos em um ambiente da AWS foi invocada a partir de um endereço IP mal-intencionado conhecido.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma operação da API S3 foi invocada a partir de um endereço IP associado a atividades mal-intencionadas conhecidas. Comumente, a API observada é associada ao

estágio de descoberta de um ataque quando um adversário está coletando informações sobre seu AWS ambiente. Exemplos incluem `GetObjectAcl` e `ListObjects`.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Discovery:S3/MaliciousIPCaller.Custom

Uma API do S3 foi invocada a partir de um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma API do S3, como `GetObjectAcl` ou `ListObjects`, foi invocada de um endereço IP incluído em uma lista de ameaças que você carregou. A lista de ameaças associada a essa descoberta está listada na seção Informações adicionais dos detalhes de uma descoberta. Esse tipo de atividade está associado ao estágio de descoberta de um ataque, no qual um invasor coleta informações para determinar se seu AWS ambiente é suscetível a um ataque mais amplo.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Discovery:S3/TorIPCaller

Uma API do S3 foi invocada a partir de um endereço IP do nó de saída do Tor.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma API do S3, como `GetObjectAcl` ou `ListObjects`, foi invocada a partir de um endereço IP do nó de saída do Tor. Esse tipo de atividade está associado ao estágio de descoberta de um ataque, no qual um invasor coleta informações para determinar se seu AWS ambiente é suscetível a um ataque mais amplo. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Isso pode indicar um acesso não autorizado aos seus recursos da AWS com a intenção de ocultar a verdadeira identidade do invasor.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Exfiltration:S3/AnomalousBehavior

Uma entidade do IAM invocou uma API do S3 de forma suspeita.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma entidade do IAM está fazendo chamadas de API que envolvem um bucket do S3 e essa atividade é diferente da linha de base estabelecida pela entidade. A chamada de API usada nessa atividade está associada ao estágio de exfiltração de um ataque, no qual um invasor tenta coletar dados. Essa atividade é suspeita porque a entidade do IAM invocou a API de uma forma incomum. Por exemplo, uma entidade do IAM sem histórico anterior invoca uma API do S3, ou uma entidade do IAM invoca uma API do S3 de um local incomum.

Essa API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. Ele rastreia vários fatores das solicitações de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, a API específica solicitada, o bucket solicitado e o número de chamadas de API feitas. Para obter mais informações sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação, consulte Como encontrar detalhes.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Exfiltration:S3/MaliciousIPCaller

Uma API do S3 comumente usada para coletar dados de um ambiente da AWS foi invocada a partir de um endereço IP mal-intencionado conhecido.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma operação da API S3 foi invocada a partir de um endereço IP associado a atividades mal-intencionadas conhecidas. Comumente, a API observada é associada a táticas de exfiltração em que um adversário está tentando coletar dados da sua rede. Exemplos incluem `GetObject` e `CopyObject`.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Impact:S3/AnomalousBehavior.Delete

Uma entidade do IAM invocou uma API do S3 que tenta excluir dados de forma suspeita.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma entidade do IAM em seu ambiente da AWS está fazendo chamadas de API que envolvem um bucket do S3, e esse comportamento difere da linha de base estabelecida pela entidade. A chamada de API usada nessa atividade está associada a um ataque

que tenta excluir dados. Essa atividade é suspeita porque a entidade do IAM invocou a API de uma forma incomum. Por exemplo, uma entidade do IAM sem histórico anterior invoca uma API do S3, ou uma entidade do IAM invoca uma API do S3 de um local incomum.

Essa API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. Ele rastreia vários fatores das solicitações de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, a API específica solicitada, o bucket solicitado e o número de chamadas de API feitas. Para obter mais informações sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação, consulte Como encontrar detalhes.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Recomendamos uma auditoria do conteúdo do seu bucket do S3 para determinar se a versão anterior do objeto pode ou deve ser restaurada.

Impact:S3/AnomalousBehavior.Permission

Uma API comumente usada para definir as permissões de lista de controle de acesso (ACL) foi invocada de forma anômala.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma entidade do IAM em seu ambiente da AWS alterou uma política de bucket ou ACL nos buckets do S3 listados. Essa alteração pode expor publicamente seus buckets do S3 a todos os usuários da AWS autenticados.

Essa API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. Ele rastreia vários fatores das solicitações de API, como o usuário que fez a solicitação, o local de onde a solicitação

foi feita, a API específica solicitada, o bucket solicitado e o número de chamadas de API feitas. Para obter mais informações sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação, consulte Como encontrar detalhes.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Recomendamos uma auditoria do conteúdo do seu bucket do S3 para garantir que nenhum objeto tenha permissão inesperada para ser acessado publicamente.

Impact:S3/AnomalousBehavior.Write

Uma entidade do IAM invocou uma API do S3 que tenta gravar dados de forma suspeita.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma entidade do IAM em seu ambiente da AWS está fazendo chamadas de API que envolvem um bucket do S3, e esse comportamento difere da linha de base estabelecida pela entidade. A chamada de API usada nessa atividade está associada a um ataque que tenta gravar dados. Essa atividade é suspeita porque a entidade do IAM invocou a API de uma forma incomum. Por exemplo, uma entidade do IAM sem histórico anterior invoca uma API do S3, ou uma entidade do IAM invoca uma API do S3 de um local incomum.

Essa API foi identificada como anômala pelo modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. Ele rastreia vários fatores das solicitações de API, como o usuário que fez a solicitação, o local de onde a solicitação foi feita, a API específica solicitada, o bucket solicitado e o número de chamadas de API feitas. Para obter mais informações sobre quais fatores da solicitação de API são incomuns para a identidade do usuário que invocou a solicitação, consulte Como encontrar detalhes.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Recomendamos uma auditoria do conteúdo do seu bucket do S3 para garantir que essa chamada de API não tenha gravado dados mal-intencionados ou não autorizados.

Impact:S3/MaliciousIPCaller

Uma API do S3 comumente usada para adulterar dados ou processos em um ambiente da AWS foi invocada a partir de um endereço IP mal-intencionado conhecido.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma operação da API S3 foi invocada a partir de um endereço IP associado a atividades mal-intencionadas conhecidas. Comumente, a API observada é associada a táticas de impacto em que um adversário está tentando manipular, interromper ou destruir dados em seu ambiente da AWS. Exemplos incluem `PutObject` e `PutObjectAcl`.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

PenTest:S3/KaliLinux

Uma API do S3 foi invocada de uma máquina Linux Kali.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma máquina executando o Kali Linux está fazendo chamadas de API do S3 usando credenciais que pertencem à sua conta da AWS. Suas credenciais podem estar

comprometidas. O Kali Linux é uma ferramenta popular de teste de penetração que profissionais de segurança usam para identificar vulnerabilidades nas instâncias do EC2 que exigem correções. Os invasores também usam essa ferramenta para encontrar vulnerabilidades na configuração do EC2 e obter acesso não autorizado ao seu ambiente da AWS.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

PenTest:S3/ParrotLinux

Uma API do S3 foi invocada a partir de uma máquina Parrot Security Linux.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma máquina executando o Parrot Security Linux está fazendo chamadas de API do S3 usando credenciais que pertencem à sua conta da AWS. Suas credenciais podem estar comprometidas. O Parrot Security Linux é uma ferramenta popular de teste de penetração que profissionais de segurança usam para identificar vulnerabilidades nas instâncias do EC2 que exigem correções. Os invasores também usam essa ferramenta para encontrar vulnerabilidades na configuração do EC2 e obter acesso não autorizado ao seu ambiente da AWS.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

PenTest:S3/PentooLinux

Uma API do S3 foi invocada de uma máquina Linux Pentoo.

Gravidade padrão: média

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma máquina executando o Pentoo Linux está fazendo chamadas de API do S3 usando credenciais que pertencem à sua conta da AWS. Suas credenciais podem estar comprometidas. O Pentoo Linux é uma ferramenta popular de teste de penetração que profissionais de segurança usam para identificar vulnerabilidades nas instâncias do EC2 que exigem correções. Os invasores também usam essa ferramenta para encontrar vulnerabilidades na configuração do EC2 e obter acesso não autorizado ao seu ambiente da AWS.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Policy:S3/AccountBlockPublicAccessDisabled

Uma entidade do IAM invocou uma API usada para desabilitar o Bloqueio de acesso público do S3 em uma conta.

Gravidade padrão: baixa

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que o Amazon S3 Block Public Access foi desabilitado no nível da conta. Quando as configurações de bloqueio de acesso público do S3 são usadas para filtrar as políticas ou listas de controle de acesso (ACLs) aplicadas ao bucket para evitar a exposição pública acidental de dados.

Normalmente, o bloqueio de acesso público do S3 é desabilitado para permitir o acesso público a um bucket ou aos objetos no bucket. Quando o S3 Block Public Access é desabilitado para uma conta, o acesso aos seus buckets é controlado pelas políticas, ACLs ou configurações de Block Public Access em nível de bucket aplicadas aos seus buckets individuais. Isso não significa necessariamente que os buckets são compartilhados publicamente, mas que você deve auditar as permissões aplicadas aos buckets para confirmar que eles fornecem o nível apropriado de acesso.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Policy:S3/BucketAnonymousAccessGranted

Uma entidade principal do IAM concedeu acesso a um bucket do S3 na Internet alterando as políticas do bucket ou as ACLs.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que o bucket do S3 listado se tornou acessível publicamente na Internet porque uma entidade do IAM alterou uma política de bucket ou ACL nesse bucket. Depois que uma alteração na política ou na ACL é detectada, usa o raciocínio automatizado desenvolvido por Zelkova para determinar se o bucket está acessível ao público.

> **Note**
>
> Se as ACLs ou políticas de bucket de um bucket estiverem configuradas para negar explicitamente ou negar tudo, essa descoberta pode não refletir o estado atual do bucket. Essa descoberta não refletirá nenhuma configuração de Bloqueio de acesso público do S3 que possa ter sido habilitada para seu bucket do S3. Nesses casos, o valor de `effectivePermission` na descoberta será marcado como `UNKNOWN`.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Policy:S3/BucketBlockPublicAccessDisabled

Uma entidade principal do IAM invocou uma API usada para desabilitar o bloqueio de acesso público do S3 em um bucket.

Gravidade padrão: baixa

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que o Bloqueio de acesso público foi desabilitado para o bucket do S3 listado. Quando habilitadas, as configurações do Bloqueio de acesso público do S3 são usadas para filtrar as políticas ou as listas de controle de acesso (ACLs) aplicadas aos buckets para evitar a exposição pública acidental de dados.

Normalmente, o bloqueio de acesso público do S3 é desabilitado para permitir o acesso público a um bucket ou aos objetos no bucket. Quando o Bloqueio de acesso público do S3 é desabilitado para um bucket, o acesso ao bucket é controlado pelas políticas ou ACLs aplicados a ele. Isso não significa que o bucket seja compartilhado publicamente, mas você deve auditar as políticas e ACLs aplicadas ao bucket para confirmar que as permissões apropriadas foram aplicadas.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Policy:S3/BucketPublicAccessGranted

Uma entidade principal do IAM concedeu acesso público a um bucket do S3 a todos os usuários da AWS alterando as políticas do bucket ou as ACLs.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que o bucket do S3 listado foi exposto publicamente a todos os usuários da AWS autenticados porque uma entidade do IAM alterou uma política de bucket ou ACL nesse bucket do S3. Depois que uma alteração na política ou na ACL é detectada, usa o raciocínio automatizado desenvolvido por Zelkova para determinar se o bucket está acessível ao público.

> **Note**
>
> Se as ACLs ou políticas de bucket de um bucket estiverem configuradas para negar explicitamente ou negar tudo, essa descoberta pode não refletir o estado atual do bucket. Essa descoberta não refletirá nenhuma configuração de Bloqueio de acesso público

do S3 que possa ter sido habilitada para seu bucket do S3. Nesses casos, o valor de `effectivePermission` na descoberta será marcado como `UNKNOWN`.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Stealth:S3/ServerAccessLoggingDisabled

O registro em log de acesso ao servidor do S3 foi desabilitado para um bucket

Gravidade padrão: baixa

- Fonte de dados: eventos CloudTrail de gerenciamento

Essa descoberta informa que o registro em log de acesso ao servidor do S3 está desabilitado para um bucket no seu ambiente da AWS. Se desativado, nenhum registro de solicitação da web será criado para qualquer tentativa de acessar o bucket do S3 identificado. No entanto, as chamadas da API de gerenciamento do S3 para o bucket, como DeleteBucket, ainda são rastreadas. Se o registro de eventos de dados do S3 estiver habilitado CloudTrail para esse bucket, as solicitações da web para objetos dentro do bucket ainda serão rastreadas. Desabilitar o registro em log é uma técnica frequentemente usada por usuários não autorizados para burlar a detecção. Para saber mais sobre os logs do S3, consulte Registro em log de acesso ao servidor do S3 e Opções de registro em log do S3.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

UnauthorizedAccess:S3/MaliciousIPCaller.Custom

Uma API do S3 foi invocada a partir de um endereço IP em uma lista de ameaças personalizada.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma operação da API do S3, por exemplo, `PutObject` ou `PutObjectAcl`, foi invocada a partir de um endereço IP incluído em uma lista de ameaças que você carregou. A lista de ameaças associada a essa descoberta está listada na seção Informações adicionais dos detalhes de uma descoberta.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

UnauthorizedAccess:S3/TorIPCaller

Uma API do S3 foi invocada a partir de um endereço IP do nó de saída do Tor.

Gravidade padrão: alta

- Fonte de dados: eventos CloudTrail de dados para S3

Essa descoberta informa que uma operação da API do S3, como `PutObject` ou `PutObjectAcl`, foi invocada a partir de um endereço IP do nó de saída do Tor. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Essa descoberta pode indicar acesso não autorizado aos seus recursos da AWS com a intenção de ocultar a verdadeira identidade do invasor.

Recomendações de correção:

Se essa atividade for inesperada para a entidade principal associada, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para ter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Tipos de descoberta desabilitados

Uma descoberta é uma notificação que contém detalhes sobre um possível problema de segurança que o GuardDuty descobre. Para obter informações sobre alterações importantes para os tipos de descoberta do GuardDuty, incluindo os tipos de descoberta recém-adicionados ou removidos, consulte Histórico de documentos da Amazon GuardDuty.

Os seguintes tipos de descoberta foram retirados e não são mais gerados pelo GuardDuty.

> **Important**
>
> NÃO é possível reativar tipos de descobertas do GuardDuty que foram retirados.

Tópicos

- UnauthorizedAccess:IAMUser/UnusualASNCaller

Exfiltration:S3/ObjectRead.Unusual

Uma entidade do IAM invocou uma API do S3 de forma suspeita.

Severidade padrão: média*

> **Note**
>
> A severidade padrão desta descoberta é Média. No entanto, se a API for invocada usando credenciais temporárias da AWS criadas em uma instância, a severidade da descoberta será Alta.

- Fonte de dados: eventos de dados do CloudTrail para S3

Essa descoberta informa que uma entidade do IAM em seu AWS ambiente está fazendo chamadas de API que envolvem um bucket do S3 e que diferem da linha de base estabelecida pela entidade. A chamada de API usada nessa atividade está associada ao estágio de exfiltração de um ataque, no qual um invasor está tentando coletar dados. Essa atividade é suspeita porque a forma como a entidade do IAM invocou a API era incomum. Por exemplo, essa entidade do IAM não tinha histórico anterior de invocação desse tipo de API, ou a API foi invocada de um local incomum.

Recomendações de correção:

Se essa atividade for inesperada para o diretor associado, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Impact:S3/PermissionsModification.Unusual

Uma entidade do IAM invocou uma API para modificar as permissões em um ou mais recursos do S3.

Severidade padrão: média*

> **Note**
>
> A severidade padrão desta descoberta é Média. No entanto, se a API for invocada usando credenciais temporárias da AWS criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta informa que uma entidade do IAM está fazendo chamadas de API projetadas para modificar as permissões em um ou mais buckets ou objetos em seu AWS ambiente. Essa ação pode ser executada por um invasor para permitir que as informações sejam compartilhadas fora da conta. Essa atividade é suspeita porque a forma como a entidade do IAM invocou a API era incomum. Por exemplo, essa entidade do IAM não tinha histórico anterior de invocação desse tipo de API, ou a API foi invocada de um local incomum.

Recomendações de correção:

Se essa atividade for inesperada para o diretor associado, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Impact:S3/ObjectDelete.Unusual

Uma entidade do IAM invocou uma API usada para excluir dados em um bucket do S3

Severidade padrão: média*

> **Note**
>
> A severidade padrão desta descoberta é Média. No entanto, se a API for invocada usando credenciais temporárias da AWS criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta informa que uma entidade específica do IAM em seu AWS ambiente está fazendo chamadas de API projetadas para excluir dados no bucket do S3 listado, excluindo o próprio bucket. Essa atividade é suspeita porque a forma como a entidade do IAM invocou a API era incomum. Por exemplo, essa entidade do IAM não tinha histórico anterior de invocação desse tipo de API, ou a API foi invocada de um local incomum.

Recomendações de correção:

Se essa atividade for inesperada para o diretor associado, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Discovery:S3/BucketEnumeration.Unusual

Uma entidade do IAM invocou uma API do S3 usada para descobrir buckets do S3 na sua rede.

Severidade padrão: média*

> **Note**
>
> A severidade padrão desta descoberta é Média. No entanto, se a API for invocada usando credenciais temporárias da AWS criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta informa que uma entidade do IAM invocou uma API do S3 para descobrir buckets do S3 em seu ambiente, como. `ListBuckets` Esse tipo de atividade está associado ao estágio de descoberta de um ataque, no qual um invasor coleta informações para determinar se seu AWS ambiente é suscetível a um ataque mais amplo. Essa atividade é suspeita porque a forma como a entidade do IAM invocou a API era incomum. Por exemplo, essa entidade do IAM não tinha histórico anterior de invocação desse tipo de API, ou a API foi invocada de um local incomum.

Recomendações de correção:

Se essa atividade for inesperada para o diretor associado, isso pode indicar que as credenciais foram expostas ou que suas permissões do S3 não são restritivas o suficiente. Para obter mais informações, consulte Corrigindo um bucket S3 potencialmente comprometido.

Persistence:IAMUser/NetworkPermissions

Uma entidade IAM invocou uma API comumente usada para alterar as permissões de acesso à rede para grupos de segurança, rotas e ACLs em sua conta da AWS.

Severidade padrão: média*

> **Note**
>
> A severidade padrão desta descoberta é Média. No entanto, se a API for invocada usando credenciais temporárias da AWS criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta indica que um diretor específico (Usuário raiz da conta da AWS, perfil do IAM ou usuário) em seu ambiente da AWS está exibindo um comportamento diferente da linha de base estabelecida. Esse principal não possui histórico prévio de invocação dessa API.

Essa descoberta é acionada quando as configurações de rede são alteradas em circunstâncias suspeitas, como quando um principal invoca a `CreateSecurityGroup` API sem nenhum histórico anterior de fazer isso. Os invasores geralmente tentam alterar os grupos de segurança para permitir determinados tráfegos de entrada em várias portas para melhorar sua capacidade de acessar uma instância do EC2.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

Persistence:IAMUser/ResourcePermissions

Uma entidade principal invocou uma API comumente usada para alterar as políticas de acesso de segurança de vários recursos em sua conta da Conta da AWS.

Severidade padrão: média*

> **Note**
>
> A severidade padrão desta descoberta é Média. No entanto, se a API for invocada usando credenciais temporárias da AWS criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta indica que um diretor específico (Usuário raiz da conta da AWS, perfil do IAM ou usuário) em seu ambiente da AWS está exibindo um comportamento diferente da linha de base estabelecida. Esse principal não possui histórico prévio de invocação dessa API.

Essa descoberta é acionada quando uma alteração é detectada nas políticas ou permissões associadas aos AWS recursos, como quando um diretor em seu AWS ambiente invoca a `PutBucketPolicy` API sem nenhum histórico anterior de fazer isso. Alguns serviços, como o Amazon S3, oferecem suporte a permissões anexadas a recursos que garantem um ou mais acessos de principais ao recurso. Com credenciais roubadas, os invasores podem alterar as políticas anexadas a um recurso, para conseguir acesso a esse recurso.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

Persistence:IAMUser/UserPermissions

Uma entidade principal invocou uma API comumente usada para adicionar, modificar ou excluir políticas, grupos ou usuários do IAM em sua conta da AWS.

Severidade padrão: média*

> **Note**
>
> A severidade padrão desta descoberta é Média. No entanto, se a API for invocada usando credenciais temporárias da AWS criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta indica que um diretor específico (Usuário raiz da conta da AWS, perfil do IAM ou usuário) em seu ambiente da AWS está exibindo um comportamento diferente da linha de base estabelecida. Esse principal não possui histórico prévio de invocação dessa API.

Essa descoberta é acionada por alterações suspeitas nas permissões relacionadas ao usuário em seu AWS ambiente, como quando um diretor em seu AWS ambiente invoca a `AttachUserPolicy` API sem nenhum histórico anterior de fazer isso. Os invasores podem usar credenciais roubadas para criar novos usuários, adicionar políticas de acesso aos usuários existentes ou criar chaves

de acesso para maximizar o acesso a uma conta, mesmo que o ponto de acesso original esteja fechado. Por exemplo, o proprietário da conta pode perceber que um determinado usuário ou senha do IAM foi roubado e excluí-lo da conta. No entanto, eles não podem excluir outros usuários que foram criados por um administrador principal criado de forma fraudulenta, deixando sua AWS conta acessível ao invasor.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

PrivilegeEscalation:IAMUser/AdministrativePermissions

Um principal tentou atribuir uma política altamente permissiva a si próprio.

Severidade padrão: baixa*

> **Note**
>
> Essa descoberta da severidade é baixa se a tenthabilita de escalonamento de privilégios não foi bem-sucedida e média se a tenthabilita de escalonamento foi bem-sucedida.

Essa descoberta indica que uma entidade do IAM específica em seu ambiente da AWS está exibindo um comportamento que pode ser indicativo de um ataque de escalonamento de privilégios. Essa descoberta é acionada quando um usuário ou perfil do IAM tenta atribuir uma política altamente permissiva a si próprio. Se o usuário ou a função não deve ter privilégios administrativos, isso indica que as credenciais do usuário foram comprometidas ou que as permissões da função podem estar configuradas inadequadamente.

Os invasores usarão credenciais roubadas para criar novos usuários, adicionar políticas de acesso aos usuários existentes ou criar chaves de acesso para maximizar o acesso a uma conta, mesmo que o ponto de acesso original esteja fechado. Por exemplo, o proprietário da conta pode perceber que a credencial de login de um determinado usuário do IAM foi roubada e excluí-lo da conta, mas pode não excluir outros usuários que foram criados por um diretor administrativo criado de forma fraudulenta, deixando sua conta da AWS ainda acessível ao invasor.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

Recon:IAMUser/NetworkPermissions

Uma entidade principal invocou uma API comumente usada para alterar as permissões de acesso de rede para grupos de segurança, rotas e ACLs em sua conta AWS.

Severidade padrão: média*

> **Note**
>
> A severidade padrão desta descoberta é Média. No entanto, se a API for invocada usando credenciais temporárias da AWS criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta indica que um diretor específico (Usuário raiz da conta da AWS, perfil do IAM ou usuário) em seu ambiente da AWS está exibindo um comportamento diferente da linha de base estabelecida. Esse principal não possui histórico prévio de invocação dessa API.

Essa descoberta é acionada quando as permissões de acesso de recurso em sua conta da AWS são examinadas quanto a circunstâncias duvidosas. Por exemplo, se uma entidade principal sem histórico de fazer isso invocou a API `DescribeInstances`. Um invasor pode usar credenciais roubadas para executar esse tipo de reconhecimento de seus recursos da AWS para localizar credenciais mais valiosas ou determinar os recursos das credenciais que já possui.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

Recon:IAMUser/ResourcePermissions

Uma entidade principal invocou uma API comumente usada para alterar as políticas de acesso de segurança de vários recursos em sua conta da AWS.

Severidade padrão: média*

> **Note**
>
> A severidade padrão desta descoberta é Média. No entanto, se a API for invocada usando credenciais temporárias da AWS criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta indica que um diretor específico (Usuário raiz da conta da AWS, perfil do IAM ou usuário) em seu ambiente da AWS está exibindo um comportamento diferente da linha de base estabelecida. Esse principal não possui histórico prévio de invocação dessa API.

Essa descoberta é acionada quando as permissões de acesso de recurso em sua conta da AWS são examinadas quanto a circunstâncias duvidosas. Por exemplo, se uma entidade principal sem histórico de fazer isso invocou a API `DescribeInstances`. Um invasor pode usar credenciais roubadas para executar esse tipo de reconhecimento de seus recursos da AWS para localizar credenciais mais valiosas ou determinar os recursos das credenciais que já possui.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

Recon:IAMUser/UserPermissions

Uma entidade principal invocou uma API comumente usada para adicionar, modificar ou excluir políticas, grupos ou usuários do IAM em sua conta da AWS.

Severidade padrão: média*

> **Note**
>
> A severidade padrão desta descoberta é Média. No entanto, se a API for invocada usando credenciais temporárias da AWS criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta é acionada quando as permissões de usuário em seu ambiente da AWS são examinadas quanto a circunstâncias duvidosas. Por exemplo, se uma entidade

principal (Usuário raiz da conta da AWS, perfil do IAM ou usuário do IAM) invocou a API `ListInstanceProfilesForRole` sem histórico de fazer isso. Um invasor pode usar credenciais roubadas para executar esse tipo de reconhecimento de seus recursos da AWS para localizar credenciais mais valiosas ou determinar os recursos das credenciais que já possui.

Essa descoberta indica que um principal específico no ambiente da AWS está exibindo um comportamento diferente da linha de base estabelecida. Esse principal não possui histórico de invocação dessa API dessa maneira.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

ResourceConsumption:IAMUser/ComputeResources

Um principal invocou uma API comumente usada para executar recursos de computação, como instâncias do EC2.

Severidade padrão: média*

> **Note**
>
> A severidade padrão desta descoberta é Média. No entanto, se a API for invocada usando credenciais temporárias da AWS criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta é acionada quando as instâncias do EC2 na conta listada em seu ambiente da AWS são iniciadas em circunstâncias suspeitas. Essa descoberta indica que um principal específico em seu AWS ambiente está exibindo um comportamento diferente da linha de base estabelecida; por exemplo, se um principal (Usuário raiz da conta da AWS, função do IAM ou usuário do IAM) invocou a `RunInstances` API sem histórico anterior de fazer isso. Isso pode ser uma indicação de um invasor usando credenciais roubadas para roubar tempo de computação (possivelmente para mineração de criptomoeda ou quebra de senhas). Também pode ser uma indicação de um invasor usando uma instância do EC2 em seu ambiente da AWS e suas credenciais para manter o acesso à sua conta.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

Stealth:IAMUser/LoggingConfigurationModified

Uma entidade principal invocou uma API comumente usada para interromper o registro em log do CloudTrail, excluir logs existentes, além de eliminar rastreamentos de atividade em sua conta da AWS.

Severidade padrão: média*

> **Note**
>
> A severidade padrão desta descoberta é Média. No entanto, se a API for invocada usando credenciais temporárias da AWS criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta é acionada quando a configuração de registro na conta da AWS listada em seu ambiente é modificada em circunstâncias suspeitas. Essa descoberta informa que um principal específico em seu AWS ambiente está exibindo um comportamento diferente da linha de base estabelecida; por exemplo, se um principal (Usuário raiz da conta da AWS, função do IAM ou usuário do IAM) invocou a `StopLogging` API sem histórico anterior de fazer isso. Isso pode ser uma indicação de um invasor tentando cobrir seus rastros eliminando qualquer traço de sua atividade.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

UnauthorizedAccess:IAMUser/ConsoleLogin

Foi observado um login de console incomum por um principal em sua conta da AWS.

Severidade padrão: média*

> **Note**
>
> A severidade padrão desta descoberta é Média. No entanto, se a API for invocada usando credenciais temporárias da AWS criadas em uma instância, a severidade da descoberta será Alta.

Essa descoberta é acionada quando um login no console é detectado em circunstâncias duvidosas. Por exemplo, se um principal sem histórico de fazer isso, invocou a API ConsoleLogin de um cliente nunca usado anteriormente ou de um local incomum. Isso pode ser uma indicação de credenciais roubadas sendo usadas para obter acesso à sua conta da AWS ou um usuário válido acessando a conta de uma maneira inválida ou menos segura (por exemplo, sem passar por uma VPN aprovada).

Essa descoberta informa que determinada entidade principal no seu ambiente da AWS está exibindo um comportamento diferente da linha de base estabelecida. Esse principal não possui histórico de atividades de login usando esse aplicativo cliente a partir desse local específico.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

UnauthorizedAccess:EC2/TorIPCaller

A instância do EC2 está recebendo conexões de entrada de um nó de saída Tor.

Severidade padrão: média

Esta descoberta informa que uma instância do EC2 no seu ambiente da AWS está recebendo conexões de entrada a partir de um nó de saída Tor. Tor é um software para permitir a comunicação anônima. Ele criptografa e aleatoriamente envia comunicações por meio de relés entre uma série de nós de rede. O último nó do Tor é chamado de nó de saída. Essa descoberta pode indicar acesso não autorizado aos seus recursos da AWS com a intenção de ocultar a verdadeira identidade do invasor.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Backdoor:EC2/XORDDOS

Uma instância do EC2 está tentando se comunicar com um endereço IP associado ao malware XorDDos.

Severidade padrão: alta

Essa descoberta informa que existe uma instância do EC2 no seu ambiente da AWS que está tentando se comunicar com um endereço IP associado ao malware XOR DDos. Essa instância do EC2 pode estar comprometida. O XOR DDoS é um malware de Trojan que sequestra sistemas Linux. Para ter acesso ao sistema, ele lança um ataque de força bruta e descobre a senha dos serviços Secure Shell (SSH) no Linux. Quando as credenciais do SSH são adquiridas e o login é realizado com sucesso, ele usa privilégios de root para executar um script que faz download e instala o XOR DDoS. Em seguida, esse malware é usado como parte de um botnet para iniciar ataques distribuídos de negação de serviço (DDoS) contra outros alvos.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

Behavior:IAMUser/InstanceLaunchUnusual

Um usuário do IAM lançou uma instância do EC2 de um tipo incomum.

Severidade padrão: alta

Essa descoberta informa que determinado usuário no seu ambiente da AWS está exibindo um comportamento diferente da linha de base estabelecida. Esse usuário não possui histórico prévio de iniciar uma instância do EC2 desse tipo. Suas credenciais podem estar comprometidas.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

CryptoCurrency:EC2/BitcoinTool.A

A instância do EC2 está se comunicando com os pools de mineração do Bitcoin.

Severidade padrão: alta

Essa descoberta informa que uma instância do EC2 no seu ambiente da AWS está se comunicando com pools de mineração do Bitcoin. No campo da mineração de criptomoeda, um pool de mineração é o agrupamento de recursos por mineiros que compartilham seu poder de processamento em uma rede para dividir o prêmio de acordo com a quantidade de trabalho que contribuíram para resolver um bloco. A menos que você use esta instância do EC2 para a mineração de Bitcoin, sua instância do EC2 pode estar comprometida.

Recomendações de correção:

Se essa atividade for inesperada, sua instância pode estar comprometida. Para obter mais informações, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

UnauthorizedAccess:IAMUser/UnusualASNCaller

Uma API foi invocada a partir de um endereço IP de uma rede incomum.

Severidade padrão: alta

Essa descoberta informa que determinada atividade foi invocada a partir de um endereço IP de uma rede incomum. Essa rede nunca foi observada em todo o histórico de uso da AWS do usuário descrito. Essa atividade pode incluir um login no console, uma tentativa de iniciar uma instância do EC2, a criação de um novo usuário do IAM ou a modificação de seus privilégios da AWS, etc. Isso pode indicar acesso não autorizado aos seus recursos da AWS.

Recomendações de correção:

Se essa atividade for inesperada, suas credenciais podem estar comprometidas. Para obter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.

Descobertas por tipo de recurso

As páginas a seguir são categorizadas por tipo de recurso associado a uma GuardDuty descoberta:

- Tipos de descoberta do EC2
- Tipos de descoberta de monitoramento de tempo de execução
- Tipos de descobertas do IAM
- Tipos de descobertas de logs de auditoria do Kubernetes
- Tipos de descoberta do Lambda Protection
- Tipos de descoberta de Malware Protection

- Tipos de descoberta do RDS Protection
- Tipos de descobertas do S3

Tabela de resultados

A tabela a seguir mostra todos os tipos de descoberta habilita classificados pela fonte de dados ou recurso fundamental, conforme aplicável. Alguns dos tipos de descoberta a seguir podem ter uma gravidade variável, indicada por um asterisco (*). Para informações sobre a gravidade variável de um tipo de descoberta, veja a descrição detalhada desse tipo de descoberta.

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
Discovery :S3/Anoma lousBehavior	Amazon S3	CloudTrail eventos de dados para S3	Baixo
Discovery:S3/ MaliciousIPCal ler	Amazon S3	CloudTrail eventos de dados para S3	Alta
Discovery:S3/ MaliciousIPCal ler.Custom	Amazon S3	CloudTrail eventos de dados para S3	Alta
Discovery:S3/ TorIPCaller	Amazon S3	CloudTrail eventos de dados para S3	Médio
Exfiltration:S3/ AnomalousBe havior	Amazon S3	CloudTrail eventos de dados para S3	Alta
Exfiltration:S3/ MaliciousIP Caller	Amazon S3	CloudTrail eventos de dados para S3	Alta
Impact:S3/ Anomalou	Amazon S3	CloudTrail eventos de dados para S3	Alta

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
sBehavior.Delete			
Impact:S3/AnomalousBehavior.Permission	Amazon S3	CloudTrail eventos de dados para S3	Alta
Impact:S3/AnomalousBehavior.Write	Amazon S3	CloudTrail eventos de dados para S3	Médio
Impact:S3/MaliciousIPCaller	Amazon S3	CloudTrail eventos de dados para S3	Alta
PenTest:S3/KaliLinux	Amazon S3	CloudTrail eventos de dados para S3	Médio
PenTest:S3/ParrotLinux	Amazon S3	CloudTrail eventos de dados para S3	Médio
PenTest:S3/PentooLinux	Amazon S3	CloudTrail eventos de dados para S3	Médio
UnauthorizedAccess:S3/TorIPCaller	Amazon S3	CloudTrail eventos de dados para S3	Alta
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	Amazon S3	CloudTrail eventos de dados para S3	Alta

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
CredentialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail evento de gestão	Médio
DefenseEvasion:IAMUser/AnomalousBehavior	IAM	CloudTrail evento de gestão	Médio
Discovery:IAMUser/AnomalousBehavior	IAM	CloudTrail evento de gestão	Baixo
Exfiltration:IAMUser/AnomalousBehavior	IAM	CloudTrail evento de gestão	Alta
Impact:IAMUser/AnomalousBehavior	IAM	CloudTrail evento de gestão	Alta
InitialAccess:IAMUser/AnomalousBehavior	IAM	CloudTrail evento de gestão	Médio
PenTest:IAMUser/KaliLinux	IAM	CloudTrail evento de gestão	Médio

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
PenTest:IAMUser/ParrotLinux	IAM	CloudTrail evento de gestão	Médio
PenTest:IAMUser/PentooLinux	IAM	CloudTrail evento de gestão	Médio
Persistence:IAMUser/AnomalousBehavior	IAM	CloudTrail evento de gestão	Médio
Stealth:IAMUser/PasswordPolicyChange	IAM	CloudTrail evento de gestão	Baixo*
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	IAM	CloudTrail evento de gestão	Alto
Policy:S3/AccountBlockPublicAccessDisabled	Amazon S3	CloudTrail evento de gestão	Baixo

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
Policy:S3/BucketAnonymousAccessGranted	Amazon S3	CloudTrail evento de gestão	Alta
Policy:S3/BucketBlockPublicAccessDisabled	Amazon S3	CloudTrail evento de gestão	Baixo
Policy:S3/BucketPublicAccessGranted	Amazon S3	CloudTrail evento de gestão	Alta
PrivilegeEscalation:IAMUser/AnomalousBehavior	IAM	CloudTrail evento de gestão	Médio
Recon:IAMUser/MaliciousIPCaller	IAM	CloudTrail evento de gestão	Médio
Recon:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail evento de gestão	Médio
Recon:IAMUser/TorIPCaller	IAM	CloudTrail evento de gestão	Médio

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
Stealth:IAMUser/CloudTrailLoggingDisabled	IAM	CloudTrail evento de gestão	Baixo
Stealth:S3/ServerAccessLoggingDisabled	Amazon S3	CloudTrail evento de gestão	Baixo
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	IAM	CloudTrail evento de gestão	Médio
UnauthorizedAccess:IAMUser/MaliciousIPCaller	IAM	CloudTrail evento de gestão	Médio
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	IAM	CloudTrail evento de gestão	Médio
UnauthorizedAccess:IAMUser/TorIPCaller	IAM	CloudTrail evento de gestão	Médio

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
Policy:IAMUser/RootCredentialUsage	IAM	CloudTrail eventos de gerenciamento ou eventos CloudTrail de dados para S3	Baixo
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	IAM	CloudTrail eventos de gerenciamento ou eventos CloudTrail de dados para S3	Alta
Backdoor:EC2/C&CActivity.B!DNS	Amazon EC2	Logs de DNS	Alta
CryptoCurrency:EC2/BitcoinTool.B!DNS	Amazon EC2	Logs de DNS	Alta
Impact:EC2/AbusedDomainRequest.Reputation	Amazon EC2	Logs de DNS	Médio
Impact:EC2/BitcoinDomainRequest.Reputation	Amazon EC2	Logs de DNS	Alta

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
Impact:EC2/MaliciousDomainRequest.Reputation	Amazon EC2	Logs de DNS	Alta
Impact:EC2/SuspiciousDomainRequest.Reputation	Amazon EC2	Logs de DNS	Baixo
Trojan:EC2/BlackholeTraffic!DNS	Amazon EC2	Logs de DNS	Médio
Trojan:EC2/DGADomainRequest.B	Amazon EC2	Logs de DNS	Alta
Trojan:EC2/DGADomainRequest.C!DNS	Amazon EC2	Logs de DNS	Alta
Trojan:EC2/DNSDataExfiltration	Amazon EC2	Logs de DNS	Alta
Trojan:EC2/DriveBySourceTraffic!DNS	Amazon EC2	Logs de DNS	Alta

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
Trojan:EC2/DropPoint!DNS	Amazon EC2	Logs de DNS	Médio
Trojan:EC2/PhishingDomainRequest!DNS	Amazon EC2	Logs de DNS	Alta
UnauthorizedAccess:EC2/MetadataDNSRebind	Amazon EC2	Logs de DNS	Alta
Execution:Container/MaliciousFile	Contêiner	Volumes do EBS	Varia de acordo com a ameaça detectada
Execution:Container/SuspiciousFile	Contêiner	Volumes do EBS	Varia de acordo com a ameaça detectada
Execution:EC2/MaliciousFile	EC2	Volumes do EBS	Varia de acordo com a ameaça detectada
Execution:EC2/SuspiciousFile	EC2	Volumes do EBS	Varia de acordo com a ameaça detectada
Execution:ECS/MaliciousFile	ECS	Volumes do EBS	Varia de acordo com a ameaça detectada

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
Execution:ECS/SuspiciousFile	ECS	Volumes do EBS	Varia de acordo com a ameaça detectada
Execution:Kubernetes/MaliciousFile	Kubernetes	Volumes do EBS	Varia de acordo com a ameaça detectada
Execution:Kubernetes/SuspiciousFile	Kubernetes	Volumes do EBS	Varia de acordo com a ameaça detectada
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	Kubernetes	Logs de auditoria do Kubernetes	Médio
CredentialAccess:Kubernetes/MaliciousIPCaller	Kubernetes	Logs de auditoria do Kubernetes	Alta
CredentialAccess:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Logs de auditoria do Kubernetes	Alta

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
CredentialAccess:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Logs de auditoria do Kubernetes	Alta
CredentialAccess:Kubernetes/TorIPCaller	Kubernetes	Logs de auditoria do Kubernetes	Alta
DefenseEvasion:Kubernetes/MaliciousIPCaller	Kubernetes	Logs de auditoria do Kubernetes	Alta
DefenseEvasion:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Logs de auditoria do Kubernetes	Alta
DefenseEvasion:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Logs de auditoria do Kubernetes	Alta
DefenseEvasion:Kubernetes/TorIPCaller	Kubernetes	Logs de auditoria do Kubernetes	Alta

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	Kubernetes	Logs de auditoria do Kubernetes	Baixo
Discovery:Kubernetes/MaliciousIPCaller	Kubernetes	Logs de auditoria do Kubernetes	Médio
Discovery:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Logs de auditoria do Kubernetes	Médio
Discovery:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Logs de auditoria do Kubernetes	Médio
Discovery:Kubernetes/TorIPCaller	Kubernetes	Logs de auditoria do Kubernetes	Médio
Execution:Kubernetes/ExecInKubeSystemPod	Kubernetes	Logs de auditoria do Kubernetes	Médio

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
Execution:Kubernetes/AnomalousBehavior.ExecInPod	Kubernetes	Logs de auditoria do Kubernetes	Médio
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	Kubernetes	Logs de auditoria do Kubernetes	Baixo
Impact:Kubernetes/MaliciousIPCaller	Kubernetes	Logs de auditoria do Kubernetes	Alta
Impact:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Logs de auditoria do Kubernetes	Alta
Impact:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Logs de auditoria do Kubernetes	Alta
Impact:Kubernetes/TorIPCaller	Kubernetes	Logs de auditoria do Kubernetes	Alta

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
Persistence:Kubernetes/ContainerWithSensitiveMount	Kubernetes	Logs de auditoria do Kubernetes	Médio
Persistence:Kubernetes/MaliciousIPCaller	Kubernetes	Logs de auditoria do Kubernetes	Médio
Persistence:Kubernetes/MaliciousIPCaller.Custom	Kubernetes	Logs de auditoria do Kubernetes	Médio
Persistence:Kubernetes/SuccessfulAnonymousAccess	Kubernetes	Logs de auditoria do Kubernetes	Alta
Persistence:Kubernetes/TorIPCaller	Kubernetes	Logs de auditoria do Kubernetes	Médio
Policy:Kubernetes/AdminAccessToDefaultServiceAccount	Kubernetes	Logs de auditoria do Kubernetes	Alta
Policy:Kubernetes/AnonymousAccessGranted	Kubernetes	Logs de auditoria do Kubernetes	Alta

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
Policy:Kubernetes/KubeflowDashboardExposed	Kubernetes	Logs de auditoria do Kubernetes	Médio
Policy:Kubernetes/ExposedDashboard	Kubernetes	Logs de auditoria do Kubernetes	Médio
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	Kubernetes	Logs de auditoria do Kubernetes	Médio*
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	Kubernetes	Logs de auditoria do Kubernetes	Baixo

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	Kubernetes	Logs de auditoria do Kubernetes	Alta
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	Kubernetes	Logs de auditoria do Kubernetes	Alta
PrivilegeEscalation:Kubernetes/PrivilegedContainer	Kubernetes	Logs de auditoria do Kubernetes	Médio
Backdoor:Lambda/C&CActivity.B	Lambda	Monitoramento de atividades da rede Lambda	Alta
CryptoCurrency:Lambda/BitcoinTool.B	Lambda	Monitoramento de atividades da rede Lambda	Alta

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
Trojan:Lambda/BlackholeTraffic	Lambda	Monitoramento de atividades da rede Lambda	Médio
Trojan:Lambda/DropPoint	Lambda	Monitoramento de atividades da rede Lambda	Médio
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	Lambda	Monitoramento de atividades da rede Lambda	Médio
UnauthorizedAccess:Lambda/TorClient	Lambda	Monitoramento de atividades da rede Lambda	Alta
UnauthorizedAccess:Lambda/TorRelay	Lambda	Monitoramento de atividades da rede Lambda	Alta
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	Bancos de dados do Amazon Aurora compatíveis	Monitoramento da atividade de login do RDS	Baixo

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	Bancos de dados do Amazon Aurora compatíveis	Monitoramento da atividade de login do RDS	Alta
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	Bancos de dados do Amazon Aurora compatíveis	Monitoramento da atividade de login do RDS	Variável
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	Bancos de dados do Amazon Aurora compatíveis	Monitoramento da atividade de login do RDS	Médio
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	Bancos de dados do Amazon Aurora compatíveis	Monitoramento da atividade de login do RDS	Alta
CredentialAccess:RDS/TorIPCaller.FailedLogin	Bancos de dados do Amazon Aurora compatíveis	Monitoramento da atividade de login do RDS	Médio
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	Bancos de dados do Amazon Aurora compatíveis	Monitoramento da atividade de login do RDS	Alta

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
Discovery:RDS/MaliciousIPCaller	Bancos de dados do Amazon Aurora compatíveis	Monitoramento da atividade de login do RDS	Médio
Discovery:RDS/TorIPCaller	Bancos de dados do Amazon Aurora compatíveis	Monitoramento da atividade de login do RDS	Médio
Backdoor:Runtime/C&CActivity.B	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta
Backdoor:Runtime/C&CActivity.B!DNS	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta
CryptoCurrency:Runtime/BitcoinTool.B	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta
CryptoCurrency:Runtime/BitcoinTool.B!DNS	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta
DefenseEvasion:Runtime/FilelessExecution	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
DefenseEvasion:Runtime/ProcessInjection.Proc	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta
DefenseEvasion:Runtime/ProcessInjection.Ptrace	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
DefenseEvasion:Runtime/ProcessInjection.VirtualMemoryWrite	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta
DefenseEvasion:Runtime/PtraceAntiDebugging	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Baixo
DefenseEvasion:Runtime/SuspiciousCommand	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta
Execution:Runtime/MaliciousFileExecuted	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta
Execution:Runtime/NewBinaryExecuted	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
Execution:Runtime/NewLibraryLoaded	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
Execution:Runtime/SuspiciousCommand	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Variável
Execution:Runtime/SuspiciousTool	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Variável
Execution:Runtime/ReverseShell	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta
Impact:Runtime/AbusedDomainRequest.Reputation	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
Impact:Runtime/BitcoinDomainRequest.Reputation	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta
Impact:Runtime/CryptoMinerExecuted	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
Impact:Runtime/MaliciousDomainRequest.Reputation	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
Impact:Runtime/SuspiciousDomainRequest.Reputation	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Baixo
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
PrivilegeEscalation:Runtime/DockerSocketAccessed	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
PrivilegeEscalation:Runtime/RuncContainerEscape	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta
PrivilegeEscalation:Runtime/UserfaultfdUsage	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
Trojan:Runtime/BlackholeTraffic	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
Trojan:Runtime/BlackholeTraffic!DNS	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
Trojan:Runtime/DropPoint	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
Trojan:Runtime/DGADomainRequest.C!DNS	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta
Trojan:Runtime/DriveBySourceTraffic!DNS	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
Trojan:Runtime/DropPoint!DNS	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Médio
Trojan:Runtime/PhishingDomainRequest!DNS	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta
UnauthorizedAccess:Runtime/MetadataDNSRebind	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta
UnauthorizedAccess:Runtime/TorClient	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta
UnauthorizedAccess:Runtime/TorRelay	Instância, cluster EKS, cluster ECS ou contêiner	Monitoramento de runtime	Alta
Backdoor:EC2/C&CActivity.B	EC2	VPC Flow Logs	Alta
Backdoor:EC2/DenialOfService.Dns	EC2	VPC Flow Logs	Alta
Backdoor:EC2/DenialOfService.Tcp	EC2	VPC Flow Logs	Alta

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
Backdoor:EC2/DenialOfService.Udp	EC2	VPC Flow Logs	Alta
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	EC2	VPC Flow Logs	Alta
Backdoor:EC2/DenialOfService.UnusualProtocol	EC2	VPC Flow Logs	Alta
Backdoor:EC2/Spambot	EC2	VPC Flow Logs	Médio
Behavior:EC2/NetworkPortUnusual	EC2	VPC Flow Logs	Médio
Behavior:EC2/TrafficVolumeUnusual	EC2	VPC Flow Logs	Médio
CryptoCurrency:EC2/BitcoinTool.B	EC2	VPC Flow Logs	Alta
DefenseEvasion:EC2/UnusualDNSResolver	EC2	VPC Flow Logs	Médio

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
DefenseEvasion:EC2/UnusualDoHActivity	EC2	VPC Flow Logs	Médio
DefenseEvasion:EC2/UnusualDoTActivity	EC2	VPC Flow Logs	Médio
Impact:EC2/PortSweep	EC2	VPC Flow Logs	Alta
Impact:EC2/WinRMBruteForce	EC2	VPC Flow Logs	Baixo*
Recon:EC2/PortProbeEMRUnprotectedPort	EC2	VPC Flow Logs	Alta
Recon:EC2/PortProbeUnprotectedPort	EC2	VPC Flow Logs	Baixo*
Recon:EC2/Portscan	EC2	VPC Flow Logs	Médio
Trojan:EC2/BlackholeTraffic	EC2	VPC Flow Logs	Médio
Trojan:EC2/DropPoint	EC2	VPC Flow Logs	Médio

Tipo de descoberta	Tipo de recurso	Fonte/atributo de dados fundamentais	Gravidade da descoberta
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	EC2	VPC Flow Logs	Médio
UnauthorizedAccess:EC2/RDPBruteForce	EC2	VPC Flow Logs	Baixo*
UnauthorizedAccess:EC2/SSHBruteForce	EC2	VPC Flow Logs	Baixo*
UnauthorizedAccess:EC2/TorClient	EC2	VPC Flow Logs	Alta
UnauthorizedAccess:EC2/TorRelay	EC2	VPC Flow Logs	Alta

Gerenciando as GuardDuty descobertas da Amazon

GuardDuty oferece vários recursos importantes para ajudá-lo a classificar, armazenar e gerenciar suas descobertas. Esses atributos ajudarão a adaptar as descobertas ao ambiente específico, reduzir o ruído resultante de descobertas de baixo valor e ajudar a manter o foco em ameaças específicas ao seu ambiente da AWS . Analise os tópicos desta página para entender como você pode usar esses recursos para aumentar o valor das descobertas GuardDuty da.

Tópicos

Criação de respostas personalizadas às GuardDuty descobertas com a Amazon CloudWatch Events

Configure notificações automáticas para GuardDuty descobertas por meio de CloudWatch eventos da Amazon. Você também pode automatizar outras tarefas por meio de CloudWatch Eventos para ajudá-lo a responder às descobertas.

Entendendo CloudWatch os registros e os motivos para ignorar recursos durante a verificação do Malware Protection

Saiba como você pode auditar os CloudWatch registros de proteção contra GuardDuty malware e quais são os motivos pelos quais sua instância do Amazon EC2 ou volumes do Amazon EBS afetados podem ter sido ignorados durante o processo de verificação.

Denunciando falsos positivos na Malware Protection do GuardDuty

Saiba mais sobre a experiência de falsos positivos na Proteção contra GuardDuty Malware e como você pode denunciar detecções de ameaças com falsos positivos.

Painel de resumo

O painel de resumo fornece uma visão agregada das GuardDuty descobertas geradas Conta da AWS na sua região atual. Atualmente, o painel comporta um volume de até 5.000 descobertas. No entanto, você pode visualizar os detalhes de todas as descobertas usando a página Descobertas no GuardDuty console ou GetFindingsou ListFindings.

> **Note**
>
> O resumo das descobertas só está disponível por meio do GuardDuty console em https://console.aws.amazon.com/guardduty/.

As seções a seguir ajudarão você a acessar o painel e entender seus componentes.

Conteúdo

- Acessar o painel Resumo
- Noções básicas sobre o painel Resumo
- Fornecendo feedback no painel Resumo

Acessar o painel Resumo

No GuardDuty console, o painel de resumo mostra uma visão consolidada das últimas 5.000 GuardDuty descobertas geradas na região atual.

Para acessar o painel Resumo

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Resumo. Quando você abre o console, GuardDuty mostra o painel de resumo.
3. Por padrão, o resumo é exibido para o mesmo dia: Hoje. O GuardDuty console oferece a opção de visualizar o resumo dos Últimos 2 dias, Últimos 7 dias e Últimos 30 dias. Para alterar o intervalo de tempo padrão, escolha uma das opções no menu suspenso acima do painel Visão geral.
4. Filtrar os dados

   - Os widgets Contas com mais descobertas, Recursos com mais descobertas e Menor ocorrência de descobertas ajudam você a filtrar os dados com base no nível de gravidade das descobertas.
   - O widget Recursos com mais descobertas também ajuda a filtrar os dados com base no tipo de recurso potencialmente afetado.

     A conta de um membro pode visualizar os detalhes do recurso potencialmente afetado que pertence à sua própria conta. Se você tiver uma conta de GuardDuty administrador e quiser ver os detalhes do recurso potencialmente afetado, abra o GuardDuty console usando as credenciais da conta de membro associada.
5. Cobertura de planos de proteção

   A cobertura dos planos de proteção fornece a contagem de contas de membros que foram ativadas GuardDuty em sua organização. As estatísticas são visíveis somente para o GuardDuty administrador delegado.

Noções básicas sobre o painel Resumo

O painel Resumo mostra os dados agregados nas seções a seguir. Antes de continuar visualizando e entendendo o resumo, certifique-se de escolher a Região da AWS desejada no seletor de região na parte superior do console. Além disso, certifique-se de escolher o intervalo de tempo desejado no

menu suspenso fornecido acima do painel Visão geral. Se nenhuma descoberta for gerada para os parâmetros escolhidos, nenhum dado estará disponível em nenhum dos widgets.

De um volume de até as últimas 5.000 GuardDuty descobertas, o painel resumido com Contas com mais descobertas, Recursos com mais descobertas e Menos descobertas que ocorrem mostra os dados com base nos 5 principais resultados. Para uma análise mais aprofundada, consulte a página Descobertas no GuardDuty console.

Visão geral

Esta seção fornece os seguintes dados:

- Total de descobertas: indica o número total de descobertas geradas em sua conta na região atual.
- Achados de alta severidade: indica o número de GuardDuty achados que têm um alto nível de severidade na região atual.
- Recursos com descobertas: indica o número de recursos associados a uma descoberta e que foram potencialmente comprometidos.
- Contas com descobertas: indica o número de contas nas quais pelo menos uma descoberta foi gerada. Se você for uma conta independente, o valor nesse campo será 1.

Para os intervalos de tempo Últimos 7 dias e Últimos 30 dias, o painel Visão geral pode mostrar a diferença percentual nas descobertas geradas semana após semana (WoW) ou mês a mês (MoM), respectivamente. Se nenhuma descoberta foi gerada na semana ou no mês anterior, sem dados para comparar, a diferença percentual pode não estar disponível.

Se você for uma conta de GuardDuty administrador, todos esses campos fornecem os dados resumidos de todas as contas de membros da sua organização.

Descobertas por gravidade

Esta seção exibe um gráfico de barras com o número total de descobertas em relação ao intervalo de tempo escolhido. Você pode visualizar o número de descobertas com gravidade baixa, média ou alta, geradas em uma data específica dentro do intervalo de tempo escolhido.

Tipos de descoberta mais comuns

Esta seção fornece uma ilustração circular dos cinco principais tipos de descobertas comuns, conforme observado em um volume de até as últimas 5.000 GuardDuty descobertas geradas na

região atual. Esse gráfico circular exibe os seguintes dados quando você passa o mouse sobre cada setor:

- Contagem de descobertas: indica o número de vezes que essa descoberta foi gerada no intervalo de tempo escolhido.
- Gravidade: indica o nível de gravidade da descoberta. Por exemplo, Média e Alta.
- Porcentagem: indica a participação desse tipo de descoberta no gráfico circular.
- Última geração: indica quanto tempo passou desde que esse tipo de descoberta foi gerado pela última vez.

Contas com a maioria das descobertas

Esta seção fornece os seguintes dados:

- Conta: indica o Conta da AWS ID em que a descoberta foi gerada.
- Contagem de descobertas: indica o número de vezes que uma descoberta foi gerada para esse ID de conta.
- Última geração: indica quanto tempo passou desde a última geração de um tipo de descoberta para esse ID de conta.
- Alta gravidade: por padrão, os dados são mostrados para os tipos de descoberta de alta gravidade. As opções possíveis para esse campo são Gravidade alta, Gravidade média e Gravidade total.

Recursos com descobertas

Esta seção fornece os seguintes dados:

- Recurso: indica o tipo de recurso potencialmente afetado e, se esse recurso pertencer à sua conta, será possível acessar o link rápido para ver os detalhes do recurso. Se você for uma conta de GuardDuty administrador, poderá visualizar os detalhes do recurso potencialmente afetado acessando o GuardDuty console com as credenciais da conta do membro à qual esse recurso pertence.
- Conta: indica a Conta da AWS ID à qual esse recurso pertence.
- Contagem de descobertas: indica o número de vezes que esse recurso foi associado a uma descoberta.

- Última geração: indica quanto tempo passou desde a última geração de um tipo de descoberta associado a esse recurso.
- Todos os tipos de recursos: por padrão, os dados são mostrados para todos os tipos de recursos. Usando o menu suspenso, você pode visualizar os dados de um tipo de recurso específico, como Instance, AccessKeyLambda e outros.
- Alta gravidade: por padrão, os dados são mostrados para os tipos de descoberta de alta gravidade. Usando o menu suspenso, é possível visualizar os dados de outros níveis de gravidade. As opções possíveis são Alta gravidade, Gravidade média e Gravidade total.

Descobertas que menos ocorrem

Esta seção fornece os detalhes dos tipos de descoberta que não são gerados com frequência em seu AWS ambiente. Esse insight pode ajudar você a investigar e agir em relação a um padrão de ameaça emergente em seu ambiente. A tabela mostra os seguintes dados:

- Tipo de descoberta: indica o nome do tipo de descoberta.
- Contagem de descobertas: indica o número de vezes que esse tipo de descoberta foi gerado no intervalo de tempo escolhido.
- Última geração: indica quanto tempo passou desde que esse tipo de descoberta foi gerado pela última vez.
- Alta gravidade: por padrão, os dados são mostrados para os tipos de descoberta de alta gravidade. As opções possíveis para esse campo são Gravidade alta, Gravidade média e Gravidade total.

Cobertura de planos de proteção

Esta seção fornece o número de contas de membros ativas que pertencem à sua organização e ativaram uma ou mais configurações de recursos e recursos adicionais (conforme aplicável) na configuração atual Região da AWS.

Somente um GuardDuty administrador delegado pode visualizar as estatísticas das contas dos membros em sua organização. Se um recurso não estiver configurado, escolha Configurar na coluna Ações.

Quando você cria uma nova AWS organização, pode levar até 24 horas para gerar as estatísticas de toda a organização.

Fornecendo feedback no painel Resumo

GuardDuty incentiva você a fornecer feedback sobre a usabilidade, os recursos e o desempenho do painel de resumo. Isso nos ajudará a melhorar o painel.

Para fornecer feedback no painel Resumo

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Resumo. Quando você abre o GuardDuty console, ele mostra o painel de resumo.
3. Selecione Feedback no canto superior direito do painel. Isso abrirá um formulário. Depois de fornecer o feedback, escolha Enviar.

Filtrar descobertas

Um filtro de descoberta permite que você visualize descobertas que correspondam aos critérios especificados e filtre quaisquer descobertas sem correspondência. Você pode criar facilmente filtros de busca usando o GuardDuty console da Amazon ou pode criá-los com a CreateFilterAPI usando JSON. Consulte as seções a seguir para entender como criar um filtro no console. Para usar esses filtros para arquivar automaticamente as descobertas recebidas, consulteRegras de supressão.

Criação de filtros no GuardDuty console

Os filtros de localização podem ser criados e testados por meio do GuardDuty console. Os filtros criados pela interface do usuário podem ser salvos para uso em regras de supressão ou em operações futuras de filtro. Um filtro é composto por pelo menos um critério de filtro, que consiste em um atributo de filtro emparelhado com pelo menos um valor.

Ao criar filtros, esteja ciente do seguinte:

- Os filtros não aceitam curingas.
- Você pode especificar no mínimo um atributo ou no máximo 50 atributos como critérios para um determinado filtro.
- Ao usar a condição igual a ou diferente de para filtrar um valor de atributo, como o ID da conta, você pode especificar um máximo de 50 valores.
- Cada atributo de critério de filtro é avaliado como um `AND` operador. Vários valores para o mesmo atributo são avaliados como`AND/OR`.

Como filtrar descobertas (console)

1. Escolha Adicionar critérios de filtro acima da lista exibida de suas GuardDuty descobertas.
2. Na lista expandida de atributos, selecione aqueles que você quer especificar como os critérios para o filtro, como ID da conta ou Tipo de ação.

> **Note**
>
> Veja a tabela de atributos de filtros nesta página para ver quais é possível usar para criar critérios de filtro.

3. No campo de texto exibido, especifique um valor para cada atributo selecionado e, em seguida, selecione Apply.

> **Note**
>
> Depois de aplicar um filtro, você pode convertê-lo para excluir descobertas correspondentes ao filtro escolhendo o ponto preto no lado esquerdo do nome do filtro. Isso cria efetivamente um filtro "diferente de" para o atributo selecionado.

4. Para salvar os atributos especificados e os respectivos valores (critérios de filtro) como um filtro, selecione Save. Forneça o nome e a descrição do filtro e escolha Done (Concluído).

Atributos do filtro

Ao criar filtros ou classificar descobertas usando as operações da API, você deve especificar critérios de filtro em JSON. Esses critérios de filtro se correlacionam com o JSON dos detalhes de uma descoberta. A tabela a seguir contém uma lista dos nomes de exibição do console para atributos de filtro e seus nomes de campo JSON equivalentes.

Nome do campo do console	Nome do campo JSON
ID da conta	accountId
ID da descoberta	id
Região	region

Nome do campo do console	Nome do campo JSON
Severidade	severity Se você usar `severity` com API,AWS CLI, ouAWS CloudFormation, ele terá um valor numérico. Para obter mais informações, consulte findingCriteria.
Tipo de descoberta	tipo
Atualizado em	updatedAt
Access Key ID	recurso. accessKeyDetails. accessKeyId
Principal ID	recurso. accessKeyDetails.ID principal
Nome de usuário	recurso. accessKeyDetails.Nome de usuário
Tipo de usuário	recurso. accessKeyDetails.Tipo de usuário
ID do perfil da instância do IAM	Resource.InstanceDetails. iamInstanceProfile .id
ID da instância	resource.instanceDetails.instanceId
ID da imagem da instância	resource.instanceDetails.imageId
Chave de tag da instância	resource.instanceDetails.tags.key
Valor de tag da instância	resource.instanceDetails.tags.value
Endereço IPv6	resource.instanceDetails.networkInterfaces.ip v6Addresses
Endereço IPv4 privado	Resource.InstanceDetails.Interfaces de rede. privateIpAddresses. privateIpAddress
Nome público do DNS	Resource.InstanceDetails.Interfaces de rede. publicDnsName

Nome do campo do console	Nome do campo JSON
IP público	resource.instanceDetails.networkInterfaces.publicIp
ID do grupo de segurança	resource.instanceDetails.networkInterfaces.securityGroups.groupId
Nome do security group	resource.instanceDetails.networkInterfaces.securityGroups.groupName
ID da sub-rede	resource.instanceDetails.networkInterfaces.subnetId
ID da VPC	resource.instanceDetails.networkInterfaces.vpcId
ARN do Outpost	resource.instanceDetails.outpostARN
Tipo de recurso	resource.resourceType
Permissões do bucket	resource.s3 .publicAccess.EffectivePermission BucketDetails
Nome do bucket	recursos.3 .name BucketDetails
Bucket tag key	resource.s3 .tags.key BucketDetails
Bucket tag value	resource.s3 .tags.value BucketDetails
Tipo de bucket	recursos.3 .type BucketDetails
Tipo de ação	service.action.actionType
API chamada	serviço.ação. awsApiCallAction.API
Tipo de chamador da API	serviço.ação. awsApiCallAction.CallerType
Códigos de erro da API	serviço.ação. awsApiCallAção.Código de erro

Nome do campo do console	Nome do campo JSON
Cidade do chamador da API	serviço.ação. awsApiCallAção. remoteIpDetails.cidade.Nome da cidade
País do chamador da API	serviço.ação. awsApiCallAção. remoteIpDetails.país.Nome do país
Endereço IPv4 do chamador da API	serviço.ação. awsApiCallAção. remoteIpDetails. Endereço IP v4
ID de ASN do chamador da API	serviço.ação. awsApiCallAção. remoteIpDetails.organização.asn
Nome de ASN do chamador da API	serviço.ação. awsApiCallAção. remoteIpDetails.organização.asnorg
Nome do serviço de chamador da API	serviço.ação. awsApiCallAction.ServiceName
Domínio de solicitação de DNS	serviço.ação. dnsRequestAction.domínio
Sufixo de domínio de solicitação de DNS	serviço.ação. dnsRequestAction. domainWithSuffix
Conexão de rede bloqueada	serviço.ação. networkConnectionAction.bloqueado
Direção de conexão de rede	serviço.ação. networkConnectionAction. Direção de conexão
Porta local de conexão de rede	serviço.ação. networkConnectionAction. localPortDetails.porta
Protocolo de conexão de rede	serviço.ação. networkConnectionAction.protocolo
Cidade de conexão de rede	serviço.ação. networkConnectionAction. remoteIpDetails.cidade.Nome da cidade

Nome do campo do console	Nome do campo JSON
País de conexão de rede	serviço.ação. networkConnectionAction. remoteIpDetails.país.Nome do país
Endereço IPv4 remoto de conexão de rede	serviço.ação. networkConnectionAction. remoteIpDetails. Endereço IP v4
ID de ASN do IP remoto de conexão de rede	serviço.ação. networkConnectionAction. remoteIpDetails.organização.asn
Nome de ASN do IP remoto de conexão de rede	serviço.ação. networkConnectionAction. remoteIpDetails.organização.asnorg
Porta remota de conexão de rede	serviço.ação. networkConnectionAction. remotePortDetails.porta
Conta remota afiliada	serviço.ação. awsApiCallAção. remoteAcc ountDetails.afiliado
Endereço IPv4 do chamador da API do Kubernetes	serviço.ação. kubernetesApiCallAção. remoteIpDetails. Endereço IP v4
Namespace do Kubernetes	serviço.ação. kubernetesApiCallAction.nam espace
ID ASN do chamador da API Kubernetes	serviço.ação. kubernetesApiCallAção. remoteIpDetails.organização.asn
URI de solicitação de chamada da API Kubernetes	serviço.ação. kubernetesApiCallAction.Req uestURI
Código de status da API do Kubernetes	serviço.ação. kubernetesApiCallCódigo de ação. Status
Endereço IPv4 local da conexão de rede	serviço.ação. networkConnectionAction. localIpDetails. Endereço IP v4
Protocolo	serviço.ação. networkConnectionAction.pro tocolo

Nome do campo do console	Nome do campo JSON
Nome do serviço de chamada de API	serviço.ação. awsApiCallAction.ServiceName
ID da conta do chamador da API	serviço.ação. awsApiCallAção. remoteAcc ountDetails.ID da conta
Nome da lista de ameaças	Serviço. Informações adicionais. threatLis tName
Função do recurso	service.resourceRole
Nome do cluster do EKS	recurso. eksClusterDetails.nome
Nome da workload do Kubernetes	Resource.KubernetesDetails. kubernete sWorkloadDetails.nome
Namespace de workload do Kubernetes	Resource.KubernetesDetails. kubernete sWorkloadDetails.namespace
Nome de usuário do Kubernetes	Resource.KubernetesDetails. kubernete sUserDetails.nome de usuário
Imagem de contêiner do Kubernetes	Resource.KubernetesDetails. kubernete sWorkloadDetails.containers.imagem
Prefixo de imagens de contêiner do Kubernetes	Resource.KubernetesDetails. kubernete sWorkloadDetails.containers.Prefixo da imagem
ID de verificação	serviço. ebsVolumeScanDetalhes. ScanID
Nome da ameaça	serviço. ebsVolumeScanDetalhes. Detecções de digitalização. threatDetectedByNome.Threat Names.Name
Gravidade da ameaça	serviço. ebsVolumeScanDetalhes. Detecções de digitalização. threatDetectedByNome.Threat Names.Severity

Nome do campo do console	Nome do campo JSON
Arquivo SHA	serviço. ebsVolumeScanDetalhes. Detecções de digitalização. threatDetectedBynome.threat names.filepaths.hash
Nome do cluster do ECS	recurso. ecsClusterDetails.nome
Imagens de contêiner do ECS	recurso. ecsClusterDetails.TaskDetails.Contai ners.Image
ARN da definição de tarefas do ECS	recurso. ecsClusterDetails.TaskDetails.Defini tionArn
Imagem de contêiner autônoma	resource.containerDetails.image
Instância de banco de dados do	recurso. rdsDbInstanceDetalhes. dbInstanc eIdentifier
ID do cluster de banco de dados	recurso. rdsDbInstanceDetalhes. dbCluster Identifier
Mecanismo do banco de dados	recurso. rdsDbInstanceDetalhes.Motor
Usuário do banco de dados	recurso. rdsDbUserDetalhes.Usuário
Chave de tags de instâncias de banco	recurso. rdsDbInstanceDetails.tags.key
Valor de tag de instância de banco de dados	recurso. rdsDbInstanceDetails.tags.value
SHA-256 executável	service.runtimedetails.process.executableSHA2 56
Nome do processo	service.runtimeDetails.process.name
Caminho executável	service.runtimeDetails.process.executablePath
Nome de função do Lambda	Resource.LambdaDetails.Nome da função
ARN da função do Lambda.	resource.lambdaDetails.functionArn

Nome do campo do console	Nome do campo JSON
Chave de tags de funções do Lambda	resource.lambdaDetails.tags.key
Valor da tag da função do Lambda	resource.lambdaDetails.tags.value
Domínio de solicitação de DNS	serviço.ação. dnsRequestAction. domainWithSuffix

Regras de supressão

Uma regra de supressão é um conjunto de critérios, que consistem em um atributo de filtro pareado com um valor, usados para filtrar descobertas arquivando automaticamente novas descobertas que correspondam aos critérios especificados. As regras de supressão podem ser usadas para filtrar descobertas de baixo valor, descobertas de falsos positivos ou ameaças nas quais você não pretende agir, para facilitar o reconhecimento das ameaças à segurança com maior impacto no ambiente.

Depois de criar uma regra de supressão, novas descobertas que correspondem aos critérios definidos na regra serão arquivadas automaticamente, desde que a regra de supressão esteja em vigor. É possível usar um filtro existente para criar uma regra de supressão ou definir um novo filtro para a regra de supressão ao criá-la. É possível configurar regras de supressão para suprimir tipos de descoberta inteiros ou definir critérios de filtro mais granulares para suprimir somente instâncias específicas de um determinado tipo de descoberta. As regras de supressão podem ser editadas a qualquer momento.

As descobertas suprimidas não são enviadas para o AWS Security Hub Amazon Simple Storage Service, o Amazon Detective ou a EventBridge Amazon, reduzindo o nível de ruído da descoberta se você GuardDuty consumir descobertas por meio do Security Hub, de um SIEM de terceiros ou de outros aplicativos de alerta e emissão de bilhetes. Se você ativouGuardDuty Proteção contra malware, as GuardDuty descobertas suprimidas não iniciarão uma verificação de malware.

GuardDuty continua gerando descobertas mesmo quando elas correspondem às suas regras de supressão, no entanto, essas descobertas são automaticamente marcadas como arquivadas. A descoberta arquivada é armazenada GuardDuty por 90 dias e pode ser visualizada a qualquer momento durante esse período. Você pode ver as descobertas suprimidas no GuardDuty console selecionando Arquivado na tabela de descobertas ou por meio da GuardDuty API usando a ListFindingsAPI com um `findingCriteria` critério `service.archived` igual a verdadeiro.

> **Note**
>
> Em um ambiente com várias contas, somente o GuardDuty administrador pode criar regras de supressão.

Casos de uso comuns para regras de supressão e exemplos

Os tipos de descoberta a seguir têm casos de uso comuns para aplicar regras de supressão, selecione o nome da descoberta para saber mais sobre essa descoberta ou revise as informações para criar uma regra de supressão para esse tipo de descoberta no console.

> **Important**
>
> GuardDuty recomenda que você crie regras de supressão de forma reativa e somente para descobertas para as quais você tenha identificado repetidamente falsos positivos.

- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS: use uma regra de supressão para arquivar automaticamente as descobertas geradas quando a rede da VPC é configurada para rotear o tráfego da Internet de modo que ele saia de um gateway on-premises, e não de um gateway da Internet da VPC.

  Essa descoberta é gerada quando a rede é configurada para rotear o tráfego da Internet de modo que ele saia de um gateway on-premises e não de um gateway da Internet (IGW) da VPC. Configurações comuns, como usar AWS Outposts, ou conexões de VPN da VPC podem resultar em tráfego roteado dessa maneira. Se esse comportamento for esperado, é recomendável usar regras de supressão no e criar uma regra que consiste em dois critérios de filtro. O primeiro critério é tipo de descoberta, que deve ser `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS`. O segundo critério de filtro é o endereço IPv4 do chamador de API com o endereço IP ou intervalo CIDR do seu gateway da Internet on-premises. O exemplo abaixo representa o filtro que você usaria para suprimir esse tipo de descoberta com base no endereço IP do chamador da API.

  ```
  Finding type: UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS
   API caller IPv4 address: 198.51.100.6
  ```

> **Note**
>
> Para incluir vários IPs de chamador de API, é possível adicionar um novo filtro de endereço IPv4 de chamador de API para cada um.

- Recon:EC2/Portscan: use uma regra de supressão para arquivar automaticamente as descobertas ao usar um aplicativo de avaliação de vulnerabilidade.

  A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `Recon:EC2/Portscan`. O segundo critério de filtro deve corresponder à instância ou às instâncias que hospedam essas ferramentas de avaliação de vulnerabilidade. É possível usar o atributo ID da imagem da instância ou o atributo de valor da Tag dependendo de quais critérios forem identificáveis com as instâncias que hospedam essas ferramentas. O exemplo abaixo representa o filtro que você usaria para suprimir esse tipo de descoberta com base em instâncias com uma determinada AMI.

  ```
  Finding type: Recon:EC2/Portscan Instance image ID: ami-999999999
  ```

- UnauthorizedAccess:EC2/SSHBruteForce: use uma regra de supressão para arquivar automaticamente as descobertas quando elas forem direcionadas a instâncias bastion.

  Se o alvo da tentativa de força bruta for um hospedeiro de bastião, isso pode representar o comportamento esperado para seu AWS ambiente. Se for esse o caso, recomendamos configurar uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `UnauthorizedAccess:EC2/SSHBruteForce`. O segundo critério de filtro deve corresponder à instância ou às instâncias que servem como um bastion host. É possível usar o atributo ID da imagem da instância ou o atributo de valor da Tag dependendo de quais critérios forem identificáveis com as instâncias que hospedam essas ferramentas. O exemplo abaixo representa o filtro que você usaria para suprimir esse tipo de descoberta com base em instâncias com um determinado valor de tag de instância.

  ```
  Finding type: UnauthorizedAccess:EC2/SSHBruteForce Instance tag value: devops
  ```

- Recon:EC2/PortProbeUnprotectedPort: use uma regra de supressão para arquivar automaticamente as descobertas quando forem elas direcionadas a instâncias intencionalmente expostas.

Pode haver casos em que instâncias são intencionalmente expostas, por exemplo, se estão hospedando servidores web. Se esse for o caso em seu AWS ambiente, recomendamos que você configure uma regra de supressão para essa descoberta. A regra de supressão deve consistir em dois critérios de filtro. O primeiro critério deve usar o atributo Tipo de descoberta com um valor de `Recon:EC2/PortProbeUnprotectedPort`. O segundo critério de filtro deve corresponder à instância ou às instâncias que servem como um bastion host. É possível usar o atributo ID da imagem da instância ou o atributo de valor da Tag dependendo de quais critérios forem identificáveis com as instâncias que hospedam essas ferramentas. O exemplo abaixo representa o filtro que você usaria para suprimir esse tipo de descoberta com base em instâncias com uma determinada chave de tag de instância no console.

```
Finding type: Recon:EC2/PortProbeUnprotectedPort Instance tag key: prod
```

Regras de supressão recomendadas para descobertas do Monitoramento de runtime do EKS

- O PrivilegeEscalation:Runtime/DockerSocketAccessed é gerado quando um processo dentro de um contêiner se comunica com o soquete do Docker. Pode haver contêineres em seu ambiente que precisem acessar o soquete do Docker por motivos legítimos. O acesso a partir desses contêineres gerará a descoberta PrivilegeEscalation:Runtime/DockerSocketAccessed. Se esse for um caso em seu AWS ambiente, recomendamos que você configure uma regra de supressão para esse tipo de descoberta. O primeiro critério deve usar o campo Tipo de descoberta com um valor igual a `PrivilegeEscalation:Runtime/DockerSocketAccessed`. O segundo critério de filtro é o campo Caminho executável com valor igual ao do processo `executablePath` na descoberta gerada. Como alternativa, o segundo critério de filtro pode usar o campo Executável SHA-256 com valor igual ao do processo `executableSha256` na descoberta gerada.
- Os clusters do Kubernetes executam seus próprios servidores DNS como pods, como `coredns`. Portanto, para cada consulta de DNS de um pod, GuardDuty captura dois eventos de DNS — um do pod e outro do pod do servidor. Isso pode gerar duplicatas para as seguintes descobertas de DNS:
  - Backdoor:Runtime/C&CActivity.B!DNS
  - CryptoCurrency:Runtime/BitcoinTool.B!DNS
  - Impact:Runtime/AbusedDomainRequest.Reputation
  - Impact:Runtime/BitcoinDomainRequest.Reputation

- Impact:Runtime/MaliciousDomainRequest.Reputation
- Impact:Runtime/SuspiciousDomainRequest.Reputation
- Trojan:Runtime/BlackholeTraffic!DNS
- Trojan:Runtime/DGADomainRequest.C!DNS
- Trojan:Runtime/DriveBySourceTraffic!DNS
- Trojan:Runtime/DropPoint!DNS
- Trojan:Runtime/PhishingDomainRequest!DNS

As descobertas duplicadas incluirão detalhes do pod, do contêiner e do processo que correspondem ao pod do seu servidor DNS. Você pode configurar uma regra de supressão para suprimir essas descobertas duplicadas usando esses campos. O primeiro critério de filtro deve usar o campo Tipo de descoberta com valor igual a um tipo de descoberta de DNS da lista de descobertas fornecida anteriormente nesta seção. O segundo critério de filtro pode ser Caminho executável com valor igual ao `executablePath` do seu servidor DNS ou Executável SHA-256 com valor igual ao `executableSHA256` do seu servidor DNS na descoberta gerada. Como terceiro critério de filtro opcional, é possível usar o campo de imagem de contêiner do Kubernetes com valor igual à imagem de contêiner do seu pod de servidor DNS na descoberta gerada.

Para criar regras de supressão em GuardDuty

Escolha seu método de acesso preferido para criar ou gerenciar regras de supressão em GuardDuty.

Console

Você pode visualizar, criar e gerenciar regras de supressão usando o GuardDuty console. As regras de supressão são geradas da mesma forma que os filtros, e seus filtros salvos existentes podem ser usados como regras de supressão. Para obter mais informações sobre como criar ARNs, consulte Filtrar descobertas.

Como criar uma regra de supressão usando o console:

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. Na página Descobertas, escolha Suprimir descobertas para abrir o painel de regras de supressão.
3. Para abrir o menu de critérios de filtro, insira o **`filter criteria`** em Adicionar critérios de filtro. Você pode escolher um critério na lista. Insira um valor válido para o critério escolhido.

> **Note**
>
> Para determinar o valor válido, visualize a tabela de descobertas e escolha uma descoberta que você deseja suprimir. Revise seus detalhes no painel de descobertas.

Você pode adicionar vários critérios de filtro e garantir que somente as descobertas apareçam na tabela que você deseja suprimir.

4. Insira um Nome e uma Descrição para a regra de supressão. Os caracteres válidos incluem ponto (.), sublinhado (_), traço (-) e caracteres alfanuméricos.
5. Escolha Salvar.

Também é possível criar uma regra de supressão a partir de um filtro já salvo. Para obter mais informações sobre como criar ARNs, consulte Filtrar descobertas.

Para criar uma regra de supressão a partir de um filtro salvo:

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. Na página Descobertas, escolha Suprimir descobertas para abrir o painel de regras de supressão.
3. No menu suspenso Regras salvas, escolha um filtro salvo.
4. Você também pode adicionar novos critérios de filtro. Se você não precisar de critérios de filtro adicionais, pule esta etapa.

   Para abrir o menu de critérios de filtro, insira o **`filter criteria`** em Adicionar critérios de filtro. Você pode escolher um critério na lista. Insira um valor válido para o critério escolhido.

   > **Note**
   >
   > Para determinar o valor válido, visualize a tabela de descobertas e escolha uma descoberta que você deseja suprimir. Revise seus detalhes no painel de descobertas.

5. Insira um Nome e uma Descrição para a regra de supressão. Os caracteres válidos incluem ponto (.), sublinhado (_), traço (-) e caracteres alfanuméricos.

6. Escolha Salvar.

Para excluir uma regra de supressão:

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. Na página Descobertas, escolha Suprimir descobertas para abrir o painel de regras de supressão.
3. No menu suspenso Regras salvas, escolha um filtro salvo.
4. Escolha Delete rule (Excluir regra).

API/CLI

Para criar uma regra de supressão usando a API:

1. Também é possível criar regras de supressão por meio da API CreateFilter. Para fazer isso, especifique os critérios de filtro em um arquivo JSON seguindo o formato do exemplo detalhado abaixo. O exemplo abaixo suprimirá qualquer descoberta não arquivada de baixa gravidade que tenha uma solicitação de DNS para o domínio test.example.com. Para descobertas de gravidade média, a lista de entrada será `["4", "5", "7"]`. Para descobertas de alta gravidade, a lista de entrada será `["6", "7", "8"]`. Você também pode filtrar com base em qualquer valor na lista.

```
{
    "Criterion": {
        "service.archived": {
            "Eq": [
                "false"
            ]
        },
        "service.action.dnsRequestAction.domain": {
            "Eq": [
                "test.example.com"
            ]
        },
        "severity": {
            "Eq": [
                "1",
                "2",
                "3"
```

```
            ]
        }
    }
}
```

Para obter uma lista de nomes de campo JSON e seus equivalentes de console, consulte Atributos do filtro.

Para testar seus critérios de filtro, use o mesmo critério JSON na API ListFindings e confirme se as descobertas corretas foram selecionadas. Para testar seus critérios de filtro usando, AWS CLI siga o exemplo usando seu próprio DetectorID e arquivo.json.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty list-findings --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
finding-criteria file://criteria.json
```

2. Carregue seu filtro para ser usado como regra de supressão com a API CreateFilter ou usando a AWS CLI seguindo o exemplo abaixo com seu próprio ID de detector, um nome para a regra de supressão e um arquivo .json.

   Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

   ```
   aws guardduty create-filter --action ARCHIVE --detector-
   id 12abc34d567e8fa901bc2d34e56789f0 --name yourfiltername --finding-criteria
    file://criteria.json
   ```

Você pode ver uma lista de seus filtros programaticamente com a API ListFilter. Você pode ver os detalhes de um filtro individual fornecendo o nome do filtro à API GetFilter. Atualize os filtros usando UpdateFilter ou exclua-os com a API DeleteFilter.

Como trabalhar com listas de IPs confiáveis e listas de ameaças

A Amazon GuardDuty monitora a segurança do seu AWS ambiente analisando e processando registros de fluxo de VPC, registros de AWS CloudTrail eventos e registros de DNS. Você pode personalizar esse escopo de monitoramento configurando GuardDuty para interromper alertas de IPs confiáveis de suas próprias listas de IP confiáveis e alertar sobre IPs maliciosos conhecidos de suas próprias listas de ameaças.

Listas de IPs confiáveis e listas de ameaças são aplicáveis somente para o tráfego destinado para endereços IP roteáveis publicamente. Os efeitos de uma lista se aplicam a todos os registros de fluxo e CloudTrail descobertas da VPC, mas não se aplicam às descobertas de DNS.

GuardDuty pode ser configurado para usar os seguintes tipos de listas.

Lista de IPs confiáveis

As listas de IP confiáveis consistem em endereços IP nos quais você confiou para comunicação segura com sua AWS infraestrutura e aplicativos. GuardDuty não gera registros de fluxo de VPC nem CloudTrail descobertas para endereços IP em listas de IP confiáveis. Você pode incluir um máximo de 2.000 endereços IP e intervalos CIDR em uma única lista de IPs confiáveis. Você pode ter somente uma lista de IPs confiáveis enviada por vez por conta da AWS e por região.

Lista de IPs de ameaças

Listas de ameaças consistem em endereços IP mal-intencionados conhecidos. Essa lista pode ser fornecida por inteligência de ameaças de terceiros ou criada especificamente para sua organização. Além de gerar descobertas devido a uma atividade potencialmente suspeita, GuardDuty também gera descobertas com base nessas listas de ameaças. Você pode incluir no máximo 250.000 endereços IP e intervalos de CIDR em uma única lista de ameaças. GuardDuty só gera descobertas com base em uma atividade que envolve endereços IP e intervalos de CIDR em suas listas de ameaças; as descobertas não são geradas com base nos nomes de domínio. A qualquer momento, você pode ter até seis listas de ameaças enviadas Conta da AWS por cada região.

> **Note**
>
> Se você incluir o mesmo IP em uma lista de IPs confiáveis e em uma lista de ameaças, ele será processado primeiro pela lista de IPs confiáveis e não vai gerar uma descoberta.

Em ambientes com várias contas, somente usuários de contas de GuardDuty administrador podem adicionar e gerenciar listas de IP confiáveis e listas de ameaças. As listas de IP confiáveis e as listas de ameaças enviadas pela conta do administrador são impostas à GuardDuty funcionalidade de suas contas de membros. Em outras palavras, nas contas dos membros, GuardDuty gera descobertas com base em atividades que envolvem endereços IP maliciosos conhecidos das listas de ameaças da conta do administrador e não gera descobertas com base em atividades que envolvem endereços IP das listas de IP confiáveis da conta do administrador. Para ter mais informações, consulte Gerenciando várias contas na Amazon GuardDuty.

Formatos das listas

GuardDuty aceita listas nos seguintes formatos.

O tamanho máximo de cada arquivo que hospeda a lista de IPs confiáveis ou a lista de ameaças é de 35 MB. Nas suas listas de ameaças e de IPs confiáveis, os endereços IP e os intervalos CIDR precisam ser inseridos em linhas separadas. Apenas os endereços IPv4 são aceitos.

- Texto sem formatação (TXT)

  Esse formato é compatível com blocos CIDR e endereços IP individuais. A seguir, veja uma lista de exemplos que usa o formato de texto sem formatação (TXT).

```
192.0.2.0/24
198.51.100.1
203.0.113.1
```

- Expressão estruturada de informações sobre ameaças (STIX)

  Esse formato é compatível com blocos CIDR e endereços IP individuais. A seguir, veja uma lista de exemplos que usa o formato STIX.

```
<?xml version="1.0" encoding="UTF-8"?>
<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:stixCommon="http://stix.mitre.org/common-1"
    xmlns:ttp="http://stix.mitre.org/TTP-1"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
```

```
    xmlns:example="http://example.com/"
    xsi:schemaLocation="
    http://stix.mitre.org/stix-1 http://stix.mitre.org/XMLSchema/core/1.2/
stix_core.xsd
    http://stix.mitre.org/Campaign-1 http://stix.mitre.org/XMLSchema/campaign/1.2/
campaign.xsd
    http://stix.mitre.org/Indicator-2 http://stix.mitre.org/XMLSchema/indicator/2.2/
indicator.xsd
    http://stix.mitre.org/TTP-2 http://stix.mitre.org/XMLSchema/ttp/1.2/ttp.xsd
    http://stix.mitre.org/default_vocabularies-1 http://stix.mitre.org/XMLSchema/
default_vocabularies/1.2.0/stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#AddressObject-2 http://cybox.mitre.org/XMLSchema/
objects/Address/2.1/Address_Object.xsd"
    id="example:STIXPackage-a78fc4e3-df94-42dd-a074-6de62babfe16"
    version="1.2">
    <stix:Observables cybox_major_version="1" cybox_minor_version="1">
        <cybox:Observable id="example:observable-80b26f43-
dc41-43ff-861d-19aff31e0236">
            <cybox:Object id="example:object-161a5438-1c26-4275-ba44-a35ba963c245">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">

 <AddressObject:Address_Valuecondition="InclusiveBetween">192.0.2.0##comma##192.0.2.255</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable id="example:observable-b442b399-aea4-436f-bb34-
b9ef6c5ed8ab">
            <cybox:Object id="example:object-b422417f-bf78-4b34-ba2d-de4b09590a6d">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>198.51.100.1</
AddressObject:Address_Value>
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
        <cybox:Observable
 id="example:observable-1742fa06-8b5e-4449-9d89-6f9f32595784">
            <cybox:Object id="example:object-dc73b749-8a31-46be-803f-71df77565391">
                <cybox:Properties xsi:type="AddressObject:AddressObjectType"
 category="ipv4-addr">
                    <AddressObject:Address_Value>203.0.113.1</
AddressObject:Address_Value>
```

```
                </cybox:Properties>
            </cybox:Object>
        </cybox:Observable>
    </stix:Observables>
</stix:STIX_Package>
```

- CSV Open Threat Exchange (OTX)™

  Esse formato é compatível com blocos CIDR e endereços IP individuais. A lista de exemplo a seguir usa o formato CSV `OTX`™.

```
Indicator type, Indicator, Description
CIDR, 192.0.2.0/24, example
IPv4, 198.51.100.1, example
IPv4, 203.0.113.1, example
```

- FireEyeCSV de inteligência de ameaças do ™ iSight

  Esse formato é compatível com blocos CIDR e endereços IP individuais. A seguir, veja uma lista de exemplo que usa um formato CSV `FireEye`™.

```
reportId, title, threatScape, audience, intelligenceType, publishDate, reportLink,
 webLink, emailIdentifier, senderAddress, senderName, sourceDomain, sourceIp,
 subject, recipient, emailLanguage, fileName, fileSize, fuzzyHash, fileIdentifier,
 md5, sha1, sha256, description, fileType, packer, userAgent, registry,
 fileCompilationDateTime, filePath, asn, cidr, domain, domainTimeOfLookup,
 networkIdentifier, ip, port, protocol, registrantEmail, registrantName, networkType,
 url, malwareFamily, malwareFamilyId, actor, actorId, observationTime

01-00000001, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000001, https://www.example.com/
report/01-00000001, , , , , , , , , , , , , , , , , , , , , , , , 192.0.2.0/24, , ,
 Related, , , , , , network, , Ursnif, 21a14673-0d94-46d3-89ab-8281a0466099, , ,
 1494944400

01-00000002, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000002, https://www.example.com/
report/01-00000002, , , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 198.51.100.1, , , , , network, , Ursnif,
 12ab7bc4-62ed-49fa-99e3-14b92afc41bf, , ,1494944400

01-00000003, Example, Test, Operational, threat, 1494944400,
 https://www.example.com/report/01-00000003, https://www.example.com/
```

```
report/01-00000003, , , , , , , , , , , , , , , , , , , , , , , , , , Related,
 203.0.113.1, , , , , network, , Ursnif, 8a78c3db-7bcb-40bc-a080-75bd35a2572d, , ,
 1494944400
```

- CSV Proofpoint™ ET Intelligence Feed

  Esse formato é compatível somente com endereços IP individuais. A lista de exemplo a seguir usa o formato CSV `Proofpoint`. O parâmetro `ports` é opcional. Se você ignorar a porta, certifique-se de deixar uma vírgula (,) no final.

```
ip, category, score, first_seen, last_seen, ports (|)
198.51.100.1, 1, 100, 2000-01-01, 2000-01-01,
203.0.113.1, 1, 100, 2000-01-01, 2000-01-01, 80
```

- AlienVaultFeed de reputação da TM

  Esse formato é compatível somente com endereços IP individuais. A lista de exemplos a seguir usa o formato `AlienVault`.

```
198.51.100.1#4#2#Malicious Host#US##0.0,0.0#3
203.0.113.1#4#2#Malicious Host#US##0.0,0.0#3
```

Permissões necessárias para fazer upload das listas de IP confiáveis e listas de ameaças

Várias identidades do IAM exigem permissões especiais para trabalhar com listas de IPs confiáveis e listas de ameaças. GuardDuty Uma identidade com a política gerenciada [AmazonGuardDutyFullAccess](#) anexada só pode renomear e desabilitar as listas de IP confiáveis e listas de ameaças carregadas.

Para conceder a várias identidades o acesso total para trabalhar com listas de IP confiáveis e listas de ameaças (além de renomear e desabilitar, isso inclui fazer upload, habilitar, excluir e atualizar a localização da lista), as seguintes ações devem estar presentes na política de permissões anexada a um usuário, um grupo ou uma função do IAM:

```
{
    "Effect": "Allow",
    "Action": [
        "iam:PutRolePolicy",
        "iam:DeleteRolePolicy"
```

```
    ],
    "Resource": "arn:aws:iam::555555555555:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
}
```

> **Important**
>
> Essas ações não estão incluídas na política gerenciada `AmazonGuardDutyFullAccess`.

Como usar criptografia no lado do servidor para listas de IP confiáveis e listas de ameaças

GuardDuty suporta os seguintes tipos de criptografia para listas: SSE-AES256 e SSE-KMS. O SSE-C não é compatível. Para obter mais informações sobre os tipos de criptografia do S3, consulte Proteger dados usando criptografia do lado do servidor.

Se sua lista for criptografada usando a criptografia SSE-KMS do lado do servidor, você deverá conceder GuardDuty à função vinculada ao serviço AWSServiceRoleForAmazonGuardDutypermissão para descriptografar o arquivo a fim de ativar a lista. Adicione a seguinte instrução à política de chaves do KMS e substitua o ID da conta pelo seu próprio:

```
{
    "Sid": "AllowGuardDutyServiceRole",
    "Effect": "Allow",
    "Principal": {
    "AWS": "arn:aws:iam::123456789123:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty"
    },
    "Action": "kms:Decrypt*",
    "Resource": "*"
}
```

Adicionar e habilitar uma lista de IPs confiáveis ou uma lista de IPs de ameaças

Escolha um dos métodos de acesso a seguir para adicionar e habilitar uma lista de IPs confiáveis ou uma lista de IPs de ameaças.

Console

(Opcional) Etapa 1: buscar o URL do local da sua lista

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. No painel de navegação, escolha Buckets.
3. Escolha o nome do bucket do Amazon S3 com a lista específica que deseja adicionar.
4. Escolha o nome do objeto (lista) para visualizar os respectivos detalhes.
5. Na guia Propriedades, copie o URI do S3 para esse objeto.

Etapa 2: adicionar uma lista de IPs confiáveis ou uma lista de ameaças

> **Important**
>
> Por padrão, em qualquer ponto no tempo, você pode ter somente uma lista de IPs confiáveis. Da mesma forma, é possível ter até seis listas de ameaças.

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Listas de domínios.
3. Na página List management, selecione Add a trusted IP list ou Add a threat list.
4. Com base na sua seleção, uma caixa de diálogo será exibida. Siga estas etapas:

   a. Em Nome da lista, insira um nome para sua lista.

      Restrições de nomenclatura da lista — O nome da sua lista pode incluir letras minúsculas, letras maiúsculas, números, traço (-) e sublinhado (_).

   b. Em Localização, informe o local em que você fez o upload da sua lista. Se você ainda não tiver configurado, consulte Step 1: Fetching location URL of your list.

      Formato do URL de localização

      - https://s3.amazonaws.com/bucket.name/file.txt
      - https://s3-aws-region.amazonaws.com/bucket.name/file.txt
      - http://bucket.s3.amazonaws.com/file.txt
      - http://bucket.s3.amazonaws.com/file.txt

- s3://bucket.name/file.txt

c. Marque a caixa de seleção I agree.

d. Escolha Add list. Por padrão, o Status da lista adicionada é Inativo. Para que a lista seja efetiva, você deve habilitá-la.

Etapa 3: habilitar uma lista de IPs confiáveis ou uma lista de ameaças

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Listas de domínios.
3. Na página Gerenciamento de listas, selecione a lista que você deseja habilitar.
4. Escolha Ações e Anexar. Pode levar até 15 minutos para que a lista entre em vigor.

API/CLI

Para listas de IP confiáveis

- Execute CreateIPSet. Certifique-se de fornecer o `detectorId` da conta-membro para a qual você deseja criar essa lista de IPs confiáveis.

  Restrições de nomenclatura da lista — O nome da sua lista pode incluir letras minúsculas, letras maiúsculas, números, traço (-) e sublinhado (_).

  - Como alternativa, você pode fazer isso executando o comando AWS Command Line Interface a seguir e certifique-se de substituir `detector-id` pelo ID do detector da conta-membro para a qual você atualizará a lista de IPs confiáveis.

```
aws guardduty create-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --name AnyOrganization List --format Plaintext --location https://
s3.amazonaws.com/DOC-EXAMPLE-BUCKET2/DOC-EXAMPLE-SOURCE-FILE.format --
activate
```

Para listas de ameaças

- Executar CreateThreatIntelSet. Certifique-se de fornecer o `detectorId` da conta-membro para a qual você deseja criar essa lista de ameaças.

- Você pode fazer isso executando o comando AWS Command Line Interface a seguir. Certifique-se de fornecer o `detectorId` da conta-membro para a qual você deseja criar uma lista de ameaças.

```
aws guardduty create-threat-intel-set --detector-
id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --
format Plaintext --location https://s3.amazonaws.com/DOC-EXAMPLE-BUCKET2/
DOC-EXAMPLE-SOURCE-FILE.format --activate
```

> **Note**
>
> Depois de ativar ou atualizar qualquer lista de IP, GuardDuty pode levar até 15 minutos para sincronizar a lista.

Para atualizar as listas de IPs confiáveis e as listas de ameaças

Você pode atualizar o nome de uma lista ou os endereços IP adicionados a uma lista que já foi adicionada e habilitada. Se você atualizar uma lista, deverá ativá-la novamente GuardDuty para usar a versão mais recente da lista.

Selecione um dos métodos de acesso para atualizar um IP confiável ou uma lista de ameaças.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Listas de domínios.
3. Na página Gerenciamento de listas, selecione o conjunto de IPs confiáveis ou uma lista de ameaças para atualizar.
4. Escolha Ações e, em seguida, escolha Editar.
5. Na caixa de diálogo Atualizar lista, atualize as informações conforme necessário.

   Restrições de nomenclatura da lista — O nome da sua lista pode incluir letras minúsculas, letras maiúsculas, números, traço (-) e sublinhado (_).
6. Selecione a caixa de seleção Eu concordo e, em seguida, selecione Atualizar lista. O valor na coluna Status mudará para Inativo.

7. Como reativar a lista atualizada

   a. Na página Gerenciamento de listas, selecione a lista que você deseja habilitar novamente.

   b. Escolha Ações e Anexar.

API/CLI

1. Execute UpdateIPSet para atualizar uma lista de IPs confiáveis.
   - Como alternativa, você pode executar o comando AWS CLI a seguir para atualizar uma lista de IPs confiáveis e certificar-se de substituir `detector-id` pelo ID de detector da conta-membro para a qual você atualizará a lista de IPs confiáveis.

   ```
   aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
    --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
   activate
   ```

2. Execute UpdateThreatIntelSet para atualizar uma lista de ameaças
   - Como alternativa, você pode executar o comando AWS CLI a seguir para atualizar uma lista de ameaças e certificar-se de substituir `detector-id` pelo ID do detector da conta do membro para a qual você atualizará a lista de ameaças.

   ```
   aws guardduty update-threatintel-set --detector-
   id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
   intel-set-id d4b94fc952d6912b8f3060768example --activate
   ```

Desabilitando ou excluindo uma lista de IPs confiáveis ou uma lista de ameaças

Escolha um dos métodos de acesso para excluir (usando o console) ou desabilitar (usando API/CLI) uma lista de IPs confiáveis ou uma lista de ameaças.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Listas de domínios.
3. Na página Gerenciamento de listas, selecione a ser excluída.

4. Escolha Ações e, em seguida, escolha Excluir.
5. Selecione Excluir e confirme a ação. A lista específica não estará mais disponível na tabela.

API/CLI

1. Para uma lista de IPs confiáveis

   Execute UpdateIPSet para atualizar uma lista de IPs confiáveis.

   - Como alternativa, você pode executar o comando AWS CLI a seguir para atualizar uma lista de IPs confiáveis e certificar-se de substituir `detector-id` pelo ID de detector da conta-membro para a qual você atualizará a lista de IPs confiáveis.

     Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

     ```
     aws guardduty update-ip-set --detector-id 12abc34d567e8fa901bc2d34e56789f0
      --name AnyOrganization List --ip-set-id d4b94fc952d6912b8f3060768example --
     no-activate
     ```

2. Para uma lista de ameaças

   Execute UpdateThreatIntelSet para atualizar uma lista de ameaças

   - Como alternativa, você pode executar o comando AWS CLI a seguir para atualizar uma lista de IPs confiáveis e certificar-se de substituir `detector-id` pelo ID do detector da conta-membro para a qual você atualizará a lista de ameaças.

     ```
     aws guardduty update-threatintel-set --detector-
     id 12abc34d567e8fa901bc2d34e56789f0 --name AnyOrganization List --threat-
     intel-set-id d4b94fc952d6912b8f3060768example --no-activate
     ```

Exportar descobertas

GuardDuty retém as descobertas geradas por um período de 90 dias. GuardDuty exporta as descobertas ativas para a Amazon EventBridge (EventBridge). Opcionalmente, você pode exportar as descobertas geradas para um bucket do Amazon Simple Storage Service (Amazon S3). Isso ajudará você a rastrear os dados históricos de atividades potencialmente suspeitas em sua conta e avaliar se as etapas de remediação recomendadas foram bem-sucedidas.

Todas as novas descobertas ativas GuardDuty geradas são exportadas automaticamente em cerca de 5 minutos após a geração da descoberta. Você pode definir a frequência com que as atualizações das descobertas ativas são exportadas para EventBridge. A frequência selecionada se aplica à exportação de novas ocorrências de descobertas existentes para EventBridge seu bucket S3 (quando configurado) e Detective (quando integrado). Para obter informações sobre como GuardDuty agrega várias ocorrências de descobertas existentes, consulte. GuardDuty encontrando agregação

Quando você define as configurações para exportar descobertas para um bucket do Amazon S3, GuardDuty usa AWS Key Management Service (AWS KMS) para criptografar os dados das descobertas em seu bucket do S3. Isso exige que você adicione permissões ao seu bucket do S3 e à AWS KMS chave para que você GuardDuty possa usá-las para exportar descobertas em sua conta.

Conteúdo

Considerações

Antes de prosseguir com os pré-requisitos e as etapas para exportar as descobertas, considere os seguintes conceitos-chave:

- As configurações de exportação são regionais — você precisa configurar as opções de exportação em cada região em que você usa GuardDuty.
- Exportar descobertas para buckets do Amazon S3 em Regiões da AWS diferentes (entre regiões) GuardDuty — suporta as seguintes configurações de exportação:
  - Seu bucket ou objeto do Amazon S3 e sua AWS KMS chave devem pertencer ao mesmo. Região da AWS
  - Para as descobertas geradas em uma região comercial, você pode optar por exportar essas descobertas para um bucket do S3 em qualquer região comercial. No entanto, você não pode exportar essas descobertas para um bucket do S3 em uma região opcional.

  - Para as descobertas geradas em uma região de aceitação, você pode optar por exportar essas descobertas para a mesma região de aceitação em que foram geradas ou para qualquer região comercial. No entanto, você não pode exportar descobertas de uma região de aceitação para outra região de aceitação.
- Permissões para exportar descobertas — Para definir as configurações para exportar descobertas ativas, seu bucket do S3 deve ter permissões que permitam GuardDuty fazer upload de objetos. Você também deve ter uma AWS KMS chave que GuardDuty possa ser usada para criptografar as descobertas.
- As descobertas arquivadas não são exportadas — o comportamento padrão é que as descobertas arquivadas, incluindo novas instâncias de descobertas suprimidas, não sejam exportadas.

  Para exportar uma descoberta arquivada, você deve desarquivá-la. Isso mudará seu status para Ativo. Com base na frequência de exportação, a descoberta será exportada para o bucket S3 configurado.
- GuardDuty a conta de administrador pode exportar descobertas geradas em contas de membros associadas — Quando você configura descobertas de exportação em uma conta de administrador, todas as descobertas das contas de membros associadas que são geradas na mesma região também são exportadas para o mesmo local que você configurou para a conta de administrador. Para ter mais informações, consulte Entendendo a relação entre a conta GuardDuty do administrador e as contas dos membros.

Etapa 1 — Permissões necessárias para exportar descobertas

Ao definir as configurações para exportar descobertas, você seleciona um bucket do Amazon S3 onde você pode armazenar as descobertas e AWS KMS uma chave para usar na criptografia de dados. Além das permissões para GuardDuty ações, você também deve ter permissões para as seguintes ações para definir com êxito as configurações para exportar descobertas:

- s3: GetBucketLocation
- s3: PutObject

Etapa 2 — Anexando a política à sua chave KMS

GuardDuty criptografa os dados de descobertas em seu bucket usando AWS Key Management Service. Para definir as configurações com êxito, primeiro você deve dar GuardDuty permissão para usar uma chave KMS. Você pode conceder as permissões anexando a política à sua chave do KMS.

Ao usar uma chave KMS de outra conta, você precisa aplicar a política de chaves fazendo login no Conta da AWS proprietário da chave. Ao definir as configurações para exportar descobertas, você também precisará do ARN da chave da conta que possui a chave.

Para modificar a política de chaves do KMS para GuardDuty criptografar suas descobertas exportadas

1. Abra o AWS KMS console em https://console.aws.amazon.com/kms.
2. Para alterar o Região da AWS, use o seletor de região no canto superior direito da página.
3. Selecione uma chave KMS existente ou execute as etapas para Criar uma nova chave no Guia do AWS Key Management Service desenvolvedor, que você usará para criptografar as descobertas exportadas.

   > **Note**
   >
   > A chave Região da AWS do KMS e o bucket do Amazon S3 devem ser iguais.

   Você pode usar o mesmo bucket do S3 e o mesmo par de chaves KMS para exportar as descobertas de qualquer região aplicável. Para obter mais informações, consulte Considerações para exportar descobertas entre regiões.
4. Na seção Key policy (Política de chaves), escolha Edit (Editar).

   Se a opção Alternar para o modo de exibição de política for exibida, escolha-a para exibir a política de chaves e, em seguida, escolha Editar.
5. Copie o seguinte bloco de política para sua política de chaves do KMS para conceder GuardDuty permissão para usar sua chave.

```
{
    "Sid": "AllowGuardDutyKey",
    "Effect": "Allow",
    "Principal": {
        "Service": "guardduty.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey",
    "Resource": "KMS key ARN",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012",
```

```
            "aws:SourceArn":
 "arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"
        }
    }
}
```

6. Edite a política substituindo os seguintes valores formatados em *vermelho* no exemplo da política:

   1. Substitua o *ARN da chave KMS* pelo Amazon Resource Name (ARN) da chave KMS. Para localizar o ARN da chave, consulte Como encontrar o ID e o ARN da chave no Guia do desenvolvedor.AWS Key Management Service
   2. Substitua *123456789012* pela Conta da AWS ID que possui a conta que exporta as descobertas. GuardDuty
   3. Substitua a *Região 2* pela região Região da AWS onde as GuardDuty descobertas são geradas.
   4. Substitua o *SourceDetectorID* pelo `detectorID` da GuardDuty conta na região específica em que as descobertas foram geradas.

      Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

   > **Note**
   >
   > Se você estiver usando GuardDuty em uma região opcional, substitua o valor do "Serviço" pelo endpoint regional dessa região. Por exemplo, se você estiver usando GuardDuty na região do Oriente Médio (Bahrein) (me-south-1), substitua por. `"Service": "guardduty.amazonaws.com"` `"Service": "guardduty.me-south-1.amazonaws.com"` Para obter informações sobre endpoints para cada região de inscrição, consulte GuardDuty endpoints e cotas.

7. Se você adicionou a declaração de política antes da declaração final, adicione uma vírgula antes de adicionar essa declaração. Certifique-se de que a sintaxe JSON da sua política de chaves do KMS seja válida.

   Selecione Salvar.

8. (Opcional) copie o ARN da chave em um bloco de notas para uso nas etapas posteriores.

Etapa 3 — Anexar a política ao bucket do Amazon S3

Adicione permissões ao bucket do Amazon S3 para o qual você exportará as descobertas para que GuardDuty possa fazer upload de objetos para esse bucket do S3. Independentemente de usar um bucket do Amazon S3 que pertença à sua conta ou a outra Conta da AWS, você deve adicionar essas permissões.

Se, em algum momento, você decidir exportar as descobertas para um bucket do S3 diferente, para continuar exportando as descobertas, você deverá adicionar permissões a esse bucket do S3 e definir as configurações de exportação das descobertas novamente.

Se você ainda não tem um bucket do Amazon S3 para o qual deseja exportar essas descobertas, consulte Criação de um bucket no Guia do usuário do Amazon S3.

Para anexar permissões à sua política de bucket do S3

1. Execute as etapas em Para criar ou editar uma política de bucket no Guia do usuário do Amazon S3, até que a página Editar política de bucket apareça.
2. O exemplo de política mostra como conceder GuardDuty permissão para exportar descobertas para seu bucket do Amazon S3. Se você alterar o caminho depois de configurar as descobertas de exportação, deverá modificar a política para conceder permissão ao novo local.

   Copie o exemplo de política a seguir e cole-o no editor de políticas do Bucket.

   Se você adicionou a declaração de política antes da declaração final, adicione uma vírgula antes de adicionar essa declaração. Certifique-se de que a sintaxe JSON da sua política de chaves do KMS seja válida.

   Exemplo de política de bucket do S3

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGuardDutygetBucketLocation",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "Amazon S3 bucket ARN",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn":
"arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "AllowGuardDutyPutObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "aws:SourceArn":
"arn:aws:guardduty:Region2:123456789012:detector/SourceDetectorID"

                }
            }
        },
        {
            "Sid": "DenyUnencryptedUploadsThis is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
        },
        {
            "Sid": "DenyIncorrectHeaderThis is optional",
            "Effect": "Deny",
            "Principal": {
```

```
                "Service": "guardduty.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption-aws-kms-key-id": "KMS key ARN"
                }
            }
        },
        {
            "Sid": "DenyNon-HTTPS",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "Amazon S3 bucket ARN/[optional prefix]/*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

3. Edite a política substituindo os seguintes valores formatados em *vermelho* no exemplo da política:

    1. Substitua o *ARN do bucket do Amazon S3* pelo Amazon Resource Name (ARN) do bucket do Amazon S3. Você pode encontrar o ARN do bucket na página Editar política do bucket no console https://console.aws.amazon.com/s3/.
    2. Substitua *123456789012* pela Conta da AWS ID que possui a conta que exporta as descobertas. GuardDuty
    3. Substitua a *Região 2* pela região Região da AWS onde as GuardDuty descobertas são geradas.
    4. Substitua o *SourceDetectorID* pelo `detectorID` da GuardDuty conta na região específica em que as descobertas foram geradas.

        Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

5. Substitua *[prefixo opcional]* parte do valor do espaço reservado *ARN/ [prefixo opcional] do bucket do S3* por um local de pasta opcional para o qual você deseja exportar as descobertas. Para obter mais informações sobre o uso de prefixos, consulte Organização de objetos usando prefixos no Guia do usuário do Amazon S3.

   Quando você fornece um local de pasta opcional que ainda não existe, GuardDuty criará esse local somente se a conta associada ao bucket do S3 for a mesma que a conta que exporta as descobertas. Quando você exporta descobertas para um bucket do S3 que pertence a outra conta, o local da pasta já deve existir.

6. Substitua o *ARN da chave KMS* pelo Amazon Resource Name (ARN) da chave KMS associada à criptografia das descobertas exportadas para o bucket do S3. Para localizar o ARN da chave, consulte Como encontrar o ID e o ARN da chave no Guia do desenvolvedor.AWS Key Management Service

> **Note**
>
> Se você estiver usando GuardDuty em uma região opcional, substitua o valor do "Serviço" pelo endpoint regional dessa região. Por exemplo, se você estiver usando GuardDuty na região do Oriente Médio (Bahrein) (me-south-1), substitua por. `"Service": "guardduty.amazonaws.com"` `"Service": "guardduty.me-south-1.amazonaws.com"` Para obter informações sobre endpoints para cada região de inscrição, consulte GuardDuty endpoints e cotas.

4. Selecione Salvar.

Etapa 4 - Exportação das descobertas para um bucket do S3 (console)

GuardDuty permite que você exporte descobertas para um bucket existente em outro Conta da AWS.

Ao criar um novo bucket do S3 ou escolher um bucket existente em sua conta, você pode adicionar um prefixo opcional. Ao configurar as descobertas de exportação, GuardDuty cria uma nova pasta no bucket do S3 para suas descobertas. O prefixo será anexado à estrutura de pastas padrão criada. GuardDuty Por exemplo, o formato do prefixo `/AWSLogs/`*`123456789012`*`/GuardDuty/`*`Region`* opcional.

> **Important**
>
> A chave do KMS e o bucket do S3 devem estar na mesma região.

Antes de concluir essas etapas, certifique-se de ter anexado as respectivas políticas à sua chave KMS e ao bucket S3 existente.

Para configurar as descobertas de exportação

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, selecione Configurações.
3. Na página Configurações, em Opções de exportação de descobertas, para o bucket do S3, escolha Configurar agora (ou Editar, conforme necessário).
4. Para o ARN do bucket do S3, insira o. **`bucket ARN`** Para encontrar o ARN do bucket, consulte Visualização das propriedades de um bucket do S3 no Guia do usuário do Amazon S3. Na guia Permissões da página de propriedades do bucket associado no console https://console.aws.amazon.com/guardduty/.
5. Para ARN da chave KMS, insira o. **`key ARN`** Para localizar o ARN da chave, consulte Como encontrar o ID e o ARN da chave no Guia do desenvolvedor.AWS Key Management Service
6. Anexar políticas
   - Execute as etapas para anexar a política de bucket do S3. Para ter mais informações, consulte Etapa 3 — Anexar a política ao bucket do Amazon S3.
   - Execute as etapas para anexar a política de chaves do KMS. Para ter mais informações, consulte Etapa 2 — Anexando a política à sua chave KMS.
7. Escolha Salvar.

Etapa 5 — Definindo a frequência para exportar descobertas ativas atualizadas

Configure a frequência de exportação de descobertas ativas atualizadas conforme apropriado para seu ambiente. Por padrão, as descobertas atualizadas são exportadas a cada 6 horas. Isso significa que todas as descobertas que forem atualizadas após a exportação mais recente serão incluídas na

próxima exportação. Se as descobertas atualizadas forem exportadas a cada 6 horas e a exportação ocorrer às 12h, todas as descobertas atualizadas após 12h serão exportadas às 18h.

Como definir a frequência

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. Escolha Configurações.
3. Na seção Opções de exportação de descobertas, selecione Frequência para descobertas atualizadas. Isso define a frequência de exportação de descobertas ativas atualizadas para o Amazon S3 EventBridge e para o Amazon S3. Você pode escolher entre as seguintes opções:
   - Atualização EventBridge e S3 a cada 15 minutos
   - Atualização EventBridge e S3 a cada 1 hora
   - Update CWE and S3 every 6 hours (default) (Atualizar o CWE e o S3 a cada 6 horas (padrão))
4. Escolha Salvar alterações.

Criação de respostas personalizadas às GuardDuty descobertas com a Amazon CloudWatch Events

GuardDuty cria um evento para a Amazon CloudWatch Events quando ocorre alguma alteração nas descobertas. Encontrar mudanças que criarão um CloudWatch evento inclui descobertas recém-geradas ou descobertas recém-agregadas. Os eventos são emitidos com base no melhor esforço.

Cada GuardDuty descoberta recebe uma ID de descoberta. GuardDuty cria um CloudWatch evento para cada descoberta com um ID de descoberta exclusivo. Todas as ocorrências subsequentes de uma descoberta existente são agregadas à descoberta inicial. Para ter mais informações, consulte GuardDuty encontrando agregação.

> **Note**
>
> Se sua conta for um administrador GuardDuty delegado, os CloudWatch eventos serão publicados em sua conta e na conta do membro em que a descoberta foi gerada.

Ao usar CloudWatch eventos com GuardDuty, você pode automatizar tarefas para ajudá-lo a responder aos problemas de segurança GuardDuty revelados pelas descobertas.

Para receber notificações sobre GuardDuty descobertas com base em CloudWatch eventos, você deve criar uma regra de CloudWatch eventos e uma meta para GuardDuty. Essa regra CloudWatch permite enviar notificações de descobertas GuardDuty geradas para o alvo especificado na regra. Para ter mais informações, consulte Criando uma regra de CloudWatch eventos e um destino para GuardDuty (CLI).

Tópicos

CloudWatch Frequência de notificação de eventos para GuardDuty

Notificações de descobertas recém-geradas com um ID de descoberta exclusivo

GuardDuty envia uma notificação com base em seu CloudWatch evento dentro de 5 minutos após a descoberta. Esse evento (e esta notificação) também inclui todas as ocorrências subsequentes dessa descoberta que ocorrem nos primeiros 5 minutos desde a descoberta com um ID exclusivo sendo gerado.

> **Note**
>
> Por padrão, a frequência das notificações sobre as descobertas recém-geradas é de cinco minutos. Essa frequência não pode ser atualizada.

Notificações para ocorrências de descoberta subsequentes

Por padrão, para cada descoberta com um ID de descoberta exclusivo, GuardDuty agrega todas as ocorrências subsequentes de um determinado tipo de descoberta que ocorrem nos intervalos de 6 horas em um único evento. GuardDuty em seguida, envia uma notificação sobre essas ocorrências subsequentes com base nesse evento. Por padrão, para as ocorrências subsequentes das descobertas existentes, GuardDuty envia notificações com base em CloudWatch eventos a cada 6 horas.

Somente uma conta de administrador pode personalizar a frequência padrão das notificações enviadas sobre a descoberta subsequente de ocorrências em CloudWatch eventos. Os usuários de contas de membro NÃO PODEM personalizar esse valor de frequência. O valor de frequência definido pela conta do administrador em sua própria conta é imposto à GuardDuty funcionalidade em todas as suas contas de membros. Se um usuário de uma conta de administrador definir esse valor de frequência como 1 hora, todas as contas de membros também terão a frequência de 1 hora de recebimento de notificações sobre as ocorrências de descoberta subsequentes. Para ter mais informações, consulte Gerenciando várias contas na Amazon GuardDuty.

> **Note**
>
> Como conta de administrador, você pode personalizar a frequência padrão das notificações sobre as ocorrências de descoberta subsequentes. Valores possíveis são 15 minutos, 1 hora ou 6 horas (padrão). Para obter informações sobre como definir a frequência dessas notificações, consulte Etapa 5 — Definindo a frequência para exportar descobertas ativas atualizadas.

Monitorando GuardDuty descobertas arquivadas com Eventos CloudWatch

Para as descobertas arquivadas manualmente, as ocorrências iniciais e todas as ocorrências subsequentes dessas descobertas (geradas após a conclusão do arquivamento) são enviadas para CloudWatch Eventos de acordo com a frequência descrita acima.

Para as descobertas arquivadas automaticamente, as ocorrências iniciais e todas as ocorrências subsequentes dessas descobertas (geradas após a conclusão do arquivamento) não são enviadas para Eventos. CloudWatch

CloudWatch formato de evento para GuardDuty

O CloudWatch evento para GuardDuty tem o seguinte formato.

```
{
 "version": "0",
 "id": "cd2d702e-ab31-411b-9344-793ce56b1bc7",
 "detail-type": "GuardDuty Finding",
 "source": "aws.guardduty",
 "account": "111122223333",
```

```
        "time": "1970-01-01T00:00:00Z",
        "region": "us-east-1",
        "resources": [],
        "detail": {GUARDDUTY_FINDING_JSON_OBJECT}
       }
```

> **Note**
>
> O valor detalhado retorna os detalhes do JSON de uma única descoberta como um objeto, em vez de retornar o valor “descobertas”, que pode suportar várias descobertas em uma matriz.

Para obter a lista completa de todos os parâmetros incluídos no `GUARDDUTY_FINDING_JSON_OBJECT`, consulte GetFindings. O parâmetro do `id` que aparece no `GUARDDUTY_FINDING_JSON_OBJECT` é o ID da descoberta descrito anteriormente.

Criação de uma regra de CloudWatch eventos para notificá-lo das GuardDuty descobertas (console)

Você pode usar o CloudWatch Events with GuardDuty para configurar alertas de busca automatizados enviando eventos de GuardDuty busca para um hub de mensagens para ajudar a aumentar a visibilidade das GuardDuty descobertas. Este tópico mostra como enviar alertas de descobertas para e-mail, Slack ou Amazon Chime configurando um tópico do SNS e, em seguida, conectando esse tópico a CloudWatch uma regra de evento de eventos.

Configurar um tópico e um endpoint do Amazon SNS

Para começar, você deve primeiro configurar um tópico no Amazon Simple Notification Service e adicionar um endpoint. Para obter mais informações, consulte Conceitos básicos no Guia do desenvolvedor do Amazon Simple Notification Service.

Esse procedimento estabelece para onde você deseja enviar os dados de GuardDuty busca. O tópico do SNS pode ser adicionado a uma regra de evento de CloudWatch eventos durante ou após a criação da regra de eventos.

Email setup

Criar um tópico do SNS

1. Faça login no console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Selecione Tópicos no painel de navegação e selecione Criar tópico.
3. Na seção Criar tópico, selecione Padrão. Em eguida, insira um Nome de tópico, por exemplo, **`GuardDuty_to_Email`**. Os outros detalhes são opcionais.
4. Selecione Criar tópico. A seção Detalhes do tópico para o novo tópico será aberta.
5. Na seção Assinatura, escolha Criar assinatura
6. a. No menu Protocolo selecione E-mail.
   b. No campo Endpoint adicione o endereço de e-mail no qual você deseja receber notificações.

   > **Note**
   >
   > Você precisa confirmar sua assinatura por meio de seu cliente de e-mail depois de criá-la.

   c. Selecione Criar assinatura
7. Verifique se há uma mensagem de assinatura em sua caixa de entrada e escolha Confirmar assinatura

Slack setup

Criar um tópico do SNS

1. Faça login no console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Selecione Tópicos no painel de navegação e selecione Criar tópico.
3. Na seção Criar tópico, selecione Padrão. Em eguida, insira um Nome de tópico, por exemplo, **`GuardDuty_to_Slack`**. Os outros detalhes são opcionais. Escolha Criar tópico para finalizar.

Configurar AWS Chatbot clientes

1. Navegue até o console do AWS Chatbot.

2. No painel Clientes configurados, selecione Configurar novo cliente.
3. Selecione Slack e confirme com “Configurar”.

> **Note**
>
> Ao escolher o Slack, você deve confirmar as permissões para o AWS Chatbot a fim de acessar seu canal selecionando “permitir”.

4. Selecione Configurar novo canal para abrir o painel de detalhes da configuração.
   a. Insira um nome para o canal.
   b. Para o canal do Slack, escolha o canal que você deseja usar. Para usar o canal privado do Slack com o AWS Chatbot, escolha Canal privado.
   c. No Slack, copie o ID do canal privado clicando com o botão direito do mouse no nome dele e selecionando Copiar link.
   d. No Console de Gerenciamento da AWS, na janela do AWS Chatbot, cole a ID que você copiou do slack no campo ID do canal privado.
   e. Em Permissões, escolha criar um perfil do IAM usando um modelo, caso ainda não tenha uma função.
   f. Em Modelos de política, escolha Permissões de notificação. Esse é o modelo de política do IAM para AWS Chatbot. Ele fornece as permissões necessárias de leitura e lista para CloudWatch alarmes, eventos e registros e para tópicos do Amazon SNS.
   g. Selecione a região na qual você criou seu tópico do SNS anteriormente e, em seguida, selecione o tópico do Amazon SNS que você criou para enviar notificações ao canal do Slack.
5. Selecione CConfigurar.

Chime setup

Criar um tópico do SNS

1. Faça login no console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Selecione Tópicos no painel de navegação e selecione Criar tópico.
3. Na seção Criar tópico, selecione Padrão. Em eguida, insira um Nome de tópico, por exemplo, **`GuardDuty_to_Chime`**. Os outros detalhes são opcionais. Escolha Criar tópico para finalizar.

Configurar AWS Chatbot clientes

1. Navegue até o console do AWS Chatbot.
2. No painel Clientes configurados, selecione Configurar novo cliente.
3. Selecione Chime e confirme com “Configurar”.
4. No painel Detalhes da configuração, insira um nome para o canal.
5. No Chime, abra a sala de bate-papo desejada
    a. Escolha o ícone de engrenagem no canto superior direito e selecione Gerenciar webhooks.
    b. Selecione Copiar URL para copiar o URL do webhook para sua área de transferência.
6. No Console de Gerenciamento da AWS, na janela do AWS Chatbot, cole o URL que você copiou no campo URL do webhook.
7. Em Permissões, escolha criar um perfil do IAM usando um modelo, caso ainda não tenha uma função.
8. Em Modelos de política, escolha Permissões de notificação. Esse é o modelo de política do IAM para AWS Chatbot. Ele fornece as permissões necessárias de leitura e lista para CloudWatch alarmes, eventos e registros e para tópicos do Amazon SNS.
9. Selecione a região na qual você criou seu tópico do SNS anteriormente e, em seguida, selecione o tópico do Amazon SNS que você criou para enviar notificações para a sala do Chime.
10. Selecione Configurar.

Configure um CloudWatch evento para GuardDuty descobertas

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. Selecione Regras no painel de navegação e escolha Criar regra.
3. No menu Nome do serviço, escolha GuardDuty.
4. No menu Tipo de evento, escolha GuardDutyEncontrar.
5. Em Visualização do padrão de evento, escolha Editar.
6. Cole o código JSON abaixo na Visualização do padrão de evento e escolha Salvar

```
{
  "source": [
```

```
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "severity": [
      4,
      4.0,
      4.1,
      4.2,
      4.3,
      4.4,
      4.5,
      4.6,
      4.7,
      4.8,
      4.9,
      5,
      5.0,
      5.1,
      5.2,
      5.3,
      5.4,
      5.5,
      5.6,
      5.7,
      5.8,
      5.9,
      6,
      6.0,
      6.1,
      6.2,
      6.3,
      6.4,
      6.5,
      6.6,
      6.7,
      6.8,
      6.9,
      7,
      7.0,
      7.1,
      7.2,
```

```
      7.3,
      7.4,
      7.5,
      7.6,
      7.7,
      7.8,
      7.9,
      8,
      8.0,
      8.1,
      8.2,
      8.3,
      8.4,
      8.5,
      8.6,
      8.7,
      8.8,
      8.9
    ]
  }
}
```

> **Note**
>
> O código acima alertará sobre qualquer descoberta média ou alta.

7. Na seção Destinos, clique em Adicionar destino.
8. No menu Selecionar destinos, escolha Tópico do SNS.
9. Em Selecionar tópico selecione o nome do tópico do SNS criado na Etapa 1.
10. Configure a entrada para o evento.

    - Se você estiver configurando notificações para o Chime ou o Slack, vá para a Etapa 11, o tipo de entrada padrão é Evento correspondente.
    - Se você estiver configurando notificações por e-mail via SNS, siga as etapas abaixo para personalizar a mensagem enviada para sua caixa de entrada usando as seguintes etapas:

    a. Expanda Configurar entrada e escolha Transformador de entrada.

    b. Copie o código a seguir e cole-o no campo Caminho de entrada.

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_description": "$.detail.description"
}
```

c. Copie o código a seguir e cole-o no campo Modelo de entrada para formatar o e-mail.

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type
 <Finding_Type> in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id%3D<Finding_ID>"
```

11. Clique em Configurar detalhes.
12. Na página Configurar detalhes da regra, insira um Nome e uma Descrição para a regra e selecione Criar regra.

Criando uma regra de CloudWatch eventos e um destino para GuardDuty (CLI)

O procedimento a seguir mostra como usar AWS CLI comandos para criar uma regra de CloudWatch eventos e um destino para GuardDuty. Especificamente, o procedimento mostra como criar uma regra que permite CloudWatch enviar eventos para todas as descobertas GuardDuty geradas e adicionar uma AWS Lambda função como destino para a regra.

> **Note**
>
> Além das funções do Lambda, GuardDuty CloudWatch oferecem suporte aos seguintes tipos de destino: instâncias do Amazon EC2, streams do Amazon Kinesis, tarefas do Amazon ECS, máquinas de estadoAWS Step Functions, o comando e destinos integrados. `run`

Você também pode criar uma regra e uma meta de CloudWatch eventos por GuardDuty meio do console de CloudWatch eventos. Para obter mais informações e etapas detalhadas, consulte Criação de uma regra de CloudWatch eventos que é acionada em um evento. Na seção Origem do evento, selecione **`GuardDuty`** para Nome do serviço e **`GuardDuty Finding`** para Tipo de evento.

Para criar uma regra e um destino

1. Para criar uma regra que permita CloudWatch enviar eventos para todas as descobertas GuardDuty geradas, execute o seguinte comando da CloudWatch CLI.

   ```
   AWS events put-rule --name Test --event-pattern "{\"source\":
   [\"aws.guardduty\"]}"
   ```

   > **Important**
   >
   > Você pode personalizar ainda mais sua regra para que ela CloudWatch instrua o envio de eventos somente para um subconjunto das descobertas GuardDuty geradas. Esse subconjunto é baseado no atributo ou nos atributos da descoberta especificado(s) na regra. Por exemplo, use o seguinte comando da CLI para criar uma regra que permite CloudWatch enviar somente eventos para as GuardDuty descobertas com a severidade de 5 ou 8:
   > ```
   > AWS events put-rule --name Test --event-pattern "{\"source\":
   > [\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"],
   > \"detail\":{\"severity\":[5,8]}}"
   > ```
   > Para isso, você pode usar qualquer um dos valores de propriedade que estão disponíveis no JSON para GuardDuty descobertas.

2. Para anexar uma função Lambda como destino para a regra que você criou na etapa 1, execute o seguinte comando da CLI CloudWatch .

```
AWS events put-targets --rule Test --targets
Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
```

> **Note**
>
> Certifique-se de substituir <your_function>o comando acima pela sua função Lambda real para os GuardDuty eventos.

3. Para adicionar as permissões necessárias para invocar o destino, execute o seguinte comando da CLI do Lambda.

```
AWS lambda add-permission --function-name <your_function> --statement-
id 1 --action 'lambda:InvokeFunction' --principal events.amazonaws.com
```

> **Note**
>
> Certifique-se de substituir <your_function>o comando acima pela sua função Lambda real para os GuardDuty eventos.

> **Note**
>
> No procedimento acima, estamos usando uma função Lambda como destino para a regra que CloudWatch aciona eventos. Você também pode configurar outros AWS recursos como alvos para acionar CloudWatch eventos. Para ter mais informações, consulte PutTargets.

CloudWatch Eventos para ambientes GuardDuty com várias contas

Como GuardDuty administrador, as regras de CloudWatch eventos em sua conta serão acionadas com base nas descobertas aplicáveis de suas contas de membros. Isso significa que, se você configurar notificações de descoberta por meio de CloudWatch Eventos em sua conta de administrador, conforme detalhado na seção anterior, você será notificado sobre descobertas de severidade alta e média geradas por suas contas de membros, além das suas próprias.

Você pode identificar a conta do membro da qual a GuardDuty descoberta se originou com o `accountId` campo dos detalhes JSON da descoberta.

Para começar a escrever uma regra de evento personalizada para uma conta-membro específica em seu ambiente no console, crie uma nova regra e cole o modelo a seguir na Visualização de padrão do evento, adicionando o ID da conta-membro que você deseja acionar o evento.

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "accountId": [
      "123456789012"
    ]
  }
}
```

> **Note**
>
> Este exemplo acionará qualquer descoberta do ID da conta listada. Vários IDs podem ser adicionados, separados por uma vírgula seguindo a sintaxe JSON.

Entendendo CloudWatch os registros e os motivos para ignorar recursos durante a verificação do Malware Protection

GuardDuty O Malware Protection publica eventos em seu grupo de CloudWatch log da Amazon /aws/guardduty/ malware-scan-events. Para cada um dos eventos relacionados à verificação de malware, é possível monitorar o status e o resultado da verificação dos recursos afetados. Alguns recursos do Amazon EC2 e volumes do Amazon EBS podem ter sido ignorados durante a verificação da Proteção contra malware.

CloudWatch Registros de auditoria na proteção GuardDuty contra malware

Há três tipos de eventos de escaneamento suportados no grupo de log malware-scan-events CloudWatch /aws/guardduty/.

Nome do evento de verificação da Proteção contra malware	Explicação
`EC2_SCAN_STARTED`	Criado quando uma proteção contra GuardDuty malware está iniciando o processo de verificaç ão de malware, como a preparação para tirar um instantâneo de um volume do EBS.
`EC2_SCAN_COMPLETED`	Criado quando a verificação do GuardDuty Malware Protection é concluída em pelo menos um dos volumes do EBS do recurso afetado. Esse evento também inclui o `snapshotId` pertencente ao volume do EBS verificado. Após a conclusão da verificação, o resultado da verificação será `CLEAN`, `THREATS_FOUND` ou `NOT_SCANNED` .
`EC2_SCAN_SKIPPED`	Criado quando o escaneamento do GuardDuty Malware Protection ignora todos os volumes do EBS do recurso afetado. Para identificar porque foram ignorados, selecione o evento correspondente e veja os detalhes. Para obter mais informações sobre os motivos para ignorar, veja Razões para ignorar o recurso durante a verificação de malware abaixo.

> **Note**
>
> Se você estiver usando umAWS Organizations, os eventos de CloudWatch registro das contas dos membros em Organizations serão publicados na conta do administrador e no grupo de registros da conta do membro.

Escolha seu método de acesso preferido para visualizar e consultar CloudWatch eventos.

Console

1. Faça login no AWS Management Console e abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, em Logs, escolha Grupos de logs. Escolha o grupo de malware-scan-events registros /aws/guardduty/ para visualizar os eventos de escaneamento da Proteção contra Malware. GuardDuty

   Para executar uma consulta, escolha Log Insights.

   Para obter informações sobre a execução de uma consulta, consulte Análise de dados de log com o CloudWatch Logs Insights no Guia CloudWatch do usuário da Amazon.
3. Escolha ID de verificação para monitorar os detalhes do recurso afetado e as descobertas do malware. Por exemplo, você pode executar a consulta a seguir para filtrar os eventos de CloudWatch log usando`scanId`. Use seu próprio *`scan-id`* válido.

   ```
   fields @timestamp, @message, scanRequestDetails.scanId as scanId
   | filter scanId like "77a6f6115da4bd95f4e4ca398492bcc0"
   | sort @timestamp asc
   ```

API/CLI

- Para trabalhar com grupos de registros, consulte Pesquisar entradas de registro usando o AWS CLI no Guia CloudWatch do usuário da Amazon.

  Escolha o grupo de malware-scan-events registros /aws/guardduty/ para visualizar os eventos de escaneamento da Proteção contra Malware. GuardDuty
- Para visualizar e filtrar eventos de log, consulte GetLogEventse FilterLogEvents, respectivamente, na Amazon CloudWatch API Reference.

GuardDuty Retenção de registros de proteção contra malware

O período padrão de retenção de registros para o grupo de registros /aws/guardduty/ é de 90 dias, após os quais os eventos de malware-scan-events registro são excluídos automaticamente. Para

alterar a política de retenção de registros para seu grupo de CloudWatch registros, consulte Alterar retenção de dados de registro em CloudWatch Registros ou PutRetentionPolicy.

Razões para ignorar o recurso durante a verificação de malware

Nos eventos relacionados à verificação de malware, alguns recursos do EC2 e volumes do EBS podem ter sido ignorados durante o processo de verificação. A tabela a seguir lista os motivos pelos quais o GuardDuty Malware Protection pode não verificar os recursos. Se aplicável, use as etapas propostas para resolver esses problemas e verifique esses recursos na próxima vez que a Proteção contra GuardDuty Malware iniciar uma verificação de malware. Os outros problemas são usados para informar você sobre o curso dos eventos e não são acionáveis.

Razões para ignorar	Explicação	Etapas propostas
`RESOURCE_NOT_FOUND`	O `resourceArn` fornecido para iniciar a verificação de malware sob demanda não foi encontrado em seu ambiente da AWS.	Valide a `resourceArn` de sua instância do Amazon EC2 ou workload de contêiner e tente novamente.
`ACCOUNT_INELIGIBLE`	A ID da AWS conta a partir da qual você tentou iniciar uma verificação de malware sob demanda não foi ativada. GuardDuty	Verifique se GuardDuty está habilitado para essa AWS conta. Quando você ativa GuardDuty um novoRegião da AWS, a sincronização pode levar até 20 minutos.
`UNSUPPORTED_KEY_ENCRYPTION`	GuardDuty O Malware Protection suporta volumes não criptografados e criptografados com a chave	Substitua a chave de criptografia por uma chave gerenciada pelo cliente. Para obter mais informaçõ

Razões para ignorar	Explicação	Etapas propostas	
	gerenciada pelo cliente. Ele não suporta a verificação de volumes do EBS que são criptografados usando a criptografia do Amazon EBS. Atualmente, há uma diferença regional em que esse motivo de salto não é aplicável. Para obter mais informações sobre elesRegiões da AWS, consulteDisponibilidade de recursos específicos da região.	es sobre os tipos de criptografia GuardDuty compatíveis, consulteVolumes do Amazon EBS compatíveis para verificação de malware.	

Razões para ignorar	Explicação	Etapas propostas	
`EXCLUDED_BY_SCAN_SETTINGS`	Durante a verificação de malware, a instância do EC2 ou o volume do EBS foi excluído. Há três possibilidades: a tag foi adicionada à lista de inclusão, mas o recurso não está associado a essa tag; a tag foi adicionada à lista de exclusão e o recurso está associado a essa tag; ou a tag `GuardDuty Excluded` está definida como `true` para esse recurso.	Atualize suas opções de verificação ou as tags associadas ao seu recurso do Amazon EC2. Para ter mais informações, consulte Opções de verificação com tags definidas pelo usuário.	
`UNSUPPORTED_VOLUME_SIZE`	O volume é maior que 1024 GB.	Não acionável.	
`NO_VOLUMES_ATTACHED`	GuardDuty A Proteção contra Malware encontrou a instância em sua conta, mas nenhum volume do EBS foi anexado a essa instância para continuar com a verificação.	Não acionável.	
`UNABLE_TO_SCAN`	É um erro de serviço interno.	Não acionável.	

Razões para ignorar	Explicação	Etapas propostas	
SNAPSHOT_NOT_FOUND	Os instantâneos criados a partir dos volumes do EBS e compartilhados com a conta de serviço não foram encontrados, e o GuardDuty Malware Protection não pôde continuar com a verificação.	Verifique CloudTrail se os instantâneos não foram removidos intencionalmente.	
SNAPSHOT_QUOTA_REACHED	Você atingiu o volume máximo permitido para snapshots em cada região. Isso evita não apenas reter, mas também criar novos snapshots.	Você pode remover snapshots antigos ou solicitar o aumento da cota. Você pode ver o limite padrão para snapshots por região e como solicitar o aumento da cota em Cotas de serviço no Guia de referência geral da AWS.	
MAX_NUMBER_OF_ATTACHED_VOLUMES_REACHED	Mais de 11 volumes do EBS foram anexados a uma instância do EC2. GuardDuty O Malware Protection examinou os primeiros 11 volumes do EBS, obtidos classificando-os em ordem alfabética. deviceName	Não acionável.	

Razões para ignorar	Explicação	Etapas propostas	
`UNSUPPORTED_PRODUCT_CODE_TYPE`	GuardDuty não suporta o escaneamento de instâncias com `productCode` as`marketplace` . Para mais informações, consulte AMIs pagas no Guia do usuário do Amazon EC2 para instâncias do Linux. Para obter mais informações, consulte `productCode` Ações de ProductCode na Referência de API do Amazon EC2.	Não acionável.	

Denunciando falsos positivos na Malware Protection do GuardDuty

Os verificaçãos do Proteção contra malware do GuardDuty podem identificar um arquivo inofensivo na sua instância ou workload do contêiner do Amazon EC2 como sendo malicioso ou prejudicial. Para melhorar sua experiência com a Malware Protection e o serviço GuardDuty, você pode denunciar resultados falsos positivos se acreditar que um arquivo identificado como malicioso ou prejudicial durante uma verificação não contém realmente malware.

Envio de arquivo falso positivo

1. Faça login no console em https://console.aws.amazon.com/guardduty.
2. Ao identificar o que parece ser um resultado falso positivo, entre em contato AWS Support para iniciar o processo de envio de um arquivo falso positivo.
3. Escolha Escaneamentos de malware.

4. Escolha um verificação para ver seu ID de busca.
5. Forneça o ID de descoberta. Você também deve fornecer o hash SHA-256 do arquivo. Isso é necessário para garantir que o Proteção contra malware do GuardDuty tenha recebido o arquivo correto.
6. A equipe do AWS Support fornecerá um URL do Amazon Simple Storage Service (S3) que você poderá usar para fazer o upload do arquivo e do hash SHA-256. Informe a AWS Support equipe depois de fazer o upload do arquivo com sucesso.

> **Warning**
>
> Não forneça diretamente o arquivo ou o hash SHA-256 para. AWS Support Você só deve fazer o upload do arquivo e do hash para o Amazon S3 por meio da URL fornecida. Se você não conseguir carregar o arquivo e o hash dentro de sete dias após o recebimento do URL, ele se tornará inválido. Se o URL se tornar inválido, você precisará entrar em contato AWS Support para receber um novo URL.

O GuardDuty mantém seu arquivo durante no máximo 30 dias. Os membros da equipe do GuardDuty analisarão seu envio e tomarão as medidas apropriadas para melhorar sua experiência com a Malware Protection e o serviço GuardDuty.

Corrigindo problemas de segurança descobertos por GuardDuty

GuardDuty A Amazon gera descobertas que indicam possíveis problemas de segurança. Nesta versão do GuardDuty, os possíveis problemas de segurança indicam uma instância do EC2 ou carga de trabalho de contêiner comprometida ou um conjunto de credenciais comprometidas em seu ambiente. AWS As seções a seguir descrevem as etapas de correção recomendadas para qualquer uma das situações. Se houver cenários alternativas de remediação, eles serão descritos na entrada desse tipo específico de descoberta. Você pode acessar as informações completas sobre um tipo de descoberta selecionando-o na tabela Tipos de descobertas ativas.

Conteúdo

Correção de uma instância potencialmente comprometida do Amazon EC2

Siga estas etapas recomendadas para corrigir uma instância do EC2 potencialmente comprometida em seu ambiente: AWS

1. Identifique a instância potencialmente comprometida do Amazon EC2

   Verifique se há malwares na instância possivelmente comprometida e remova todos aqueles que forem descobertos. Você pode usar a Verificação de malware sob demanda para identificar

malware na instância EC2 potencialmente comprometida ou verificar o AWS Marketplace para conferir se há produtos parceiros úteis para identificar e remover malware.

2. Isole a instância potencialmente comprometida do Amazon EC2

   Se possível, use as etapas a seguir para isolar a instância potencialmente comprometida:

   1. Crie um grupo de segurança de isolamento dedicado.
   2. Crie uma única regra de `0.0.0.0/0 (0-65535)` para todo o tráfego nas regras de saída.

      Quando essa regra se aplica, ela converterá todo o tráfego de saída existente (e novo) em não rastreado, bloqueando todas as sessões de saída estabelecidas. Para obter mais informações, consulte Conexões não rastreadas.
   3. Remova todas as associações atuais de grupos de segurança da instância potencialmente comprometida.
   4. Associe o grupo de segurança Isolation a essa instância.

      Depois de associar, exclua a regra `0.0.0.0/0 (0-65535)` para todo o tráfego das regras de saída do grupo de segurança Isolation.

3. Identifique a origem da atividade suspeita

   Se for detectado um malware, com base no tipo de descoberta em sua conta, identifique e interrompa a atividade potencialmente não autorizada em sua instância do EC2. Isso pode exigir medidas como fechar todas as portas abertas, alterar as políticas de acesso e atualizar aplicações para corrigir as vulnerabilidades.

   Se você não conseguir identificar e interromper atividades não autorizadas em sua instância do EC2 potencialmente comprometida, recomendamos que você encerre a instância do EC2 comprometida e a substitua por uma nova instância, conforme necessário. Veja a seguir os recursos adicionais para proteger suas instâncias do EC2:

   - Seções Segurança e Rede em Melhores práticas do Amazon EC2.
   - Grupos de segurança do Amazon EC2 para instâncias do Linux e Grupos de segurança do Amazon EC2 para instâncias do Windows
   - Segurança no Amazon EC2
   - Tips for securing your EC2 instances (Linux) (Dicas para proteger as instâncias do EC2 (Linux)).
   - AWS melhores práticas de segurança
   - Incidentes no domínio da infraestrutura em AWS

4. Navegar AWS re:Post

   Navegue AWS re:Post em https://forums.aws.amazon.com/index.jspa para obter mais assistência.

5. Envie uma solicitação de suporte técnico

   Se você for assinante do pacote Premium Support, poderá enviar uma solicitação de suporte técnico.

Corrigindo um bucket S3 potencialmente comprometido

Siga estas etapas recomendadas para corrigir um bucket Amazon S3 potencialmente comprometido em seu ambiente: AWS

1. Identifique o recurso S3 potencialmente comprometido.

   Uma GuardDuty descoberta para o S3 listará o bucket do S3 associado, seu Amazon Resource Name (ARN) e seu proprietário nos detalhes da descoberta.

2. Identifique a origem da atividade suspeita e a chamada de API usada.

   A chamada de API usada será listada como `API` nos detalhes da descoberta. A origem será uma entidade principal do IAM (um perfil, um usuário ou uma conta do IAM) e os detalhes de identificação serão listados na descoberta. Dependendo do tipo de origem, o endereço IP remoto ou as informações do domínio de origem estarão disponíveis e poderão ajudar você a avaliar se a origem foi autorizada. Se a descoberta envolver credenciais de uma instância do Amazon EC2, os detalhes desse recurso também serão incluídos.

3. Determine se a origem da chamada foi autorizada a acessar o recurso identificado.

   Por exemplo, considere o seguinte:

   - Se um usuário do IAM estava envolvido, é possível que suas credenciais tenham sido potencialmente comprometidas? Para ter mais informações, consulte Correção de credenciais potencialmente comprometidas AWS.
   - Se uma API foi invocada por uma entidade principal sem histórico anterior de invocação desse tipo de API, essa origem precisa de permissões de acesso tal operação? É possível restringir ainda mais as permissões do bucket?
   - Se o acesso foi visto a partir do nome de usuário `ANONYMOUS_PRINCIPAL` com o tipo de usuário `AWSAccount`, isso indica que o bucket é público e foi acessado. Esse bucket deveria

ser público? Se a resposta for não, revise as recomendações de segurança abaixo a fim de encontrar soluções alternativas para compartilhar recursos do S3.

- Se o acesso foi feito por meio de uma chamada `PreflightRequest` bem-sucedida vista do nome de usuário `ANONYMOUS_PRINCIPAL` com o tipo de usuário `AWSAccount`, isso indica que o bucket tem uma política de compartilhamento de recursos de origem cruzada (CORS) definida. Esse bucket deve ter uma política de CORS? Se a resposta for não, certifique-se de que o bucket não esteja designado como público por engano e analise as recomendações de segurança abaixo a fim de encontrar soluções alternativas para compartilhar recursos do S3. Para obter mais informações sobre o CORS, consulte Usar o compartilhamento de recursos de origem cruzada (CORS) no guia do usuário do S3.

4. Determine se o bucket do S3 contém dados confidenciais.

   Use o Amazon Macie para determinar se o bucket do S3 contém dados confidenciais, como informações de identificação pessoal (PII), dados financeiros ou credenciais. Se a descoberta automatizada de dados confidenciais estiver habilitada para sua conta do Macie, revise os detalhes do bucket do S3 a fim de entender melhor o conteúdo do bucket do S3. Se esse atributo estiver desabilitado em sua conta do Macie, recomendamos habilitá-lo para agilizar sua avaliação. Outra alternativa é criar e executar um trabalho de descoberta de dados confidenciais para inspecionar os objetos do bucket do S3 em busca de dados confidenciais. Para obter mais informações, consulte Discovering sensitive data with Amazon Macie.

A descoberta pode ser ignorada se o acesso foi autorizado. O console https://console.aws.amazon.com/guardduty/ permite configurar regras para suprimir totalmente as descobertas individuais e impedir sua exibição. Para ter mais informações, consulte Regras de supressão.

Se você determinar que seus dados do S3 foram expostos ou acessados por uma parte não autorizada, revise as seguintes recomendações de segurança do S3 para aumentar as permissões e restringir o acesso. As soluções de remediação apropriadas serão determinadas pelas necessidades de seu ambiente específico.

Recomendações com base nas necessidades específicas de acesso ao bucket do S3

A lista a seguir fornece recomendações com base nas necessidades específicas de acesso ao bucket do Amazon S3:

- Para uma forma centralizada de limitar o acesso público ao uso de dados do S3, o S3 bloqueia o acesso público. As configurações de bloqueio de acesso público podem ser ativadas para pontos de acesso, buckets e AWS contas por meio de quatro configurações diferentes para controlar a granularidade do acesso. Para obter mais informações, consulte Configurações do bloqueio de acesso público do S3.
- AWS As políticas de acesso podem ser usadas para controlar como os usuários do IAM podem acessar seus recursos ou como seus buckets podem ser acessados. Para obter mais informações, consulte Políticas de bucket e políticas de usuário.

  Além disso, você pode usar endpoints da nuvem privada virtual (VPC) com políticas de bucket do S3 para restringir o acesso a endpoints da VPC específicos. Veja mais informações em Exemplos de políticas de buckets para endpoints da VPC do Amazon S3
- Para permitir que entidades confiáveis fora de sua conta acessem temporariamente os objetos do S3, é possível criar um URL pré-assinado por meio do S3. Esse acesso é criado com as credenciais da sua conta e, dependendo das credenciais usadas, pode durar de 6 horas a 7 dias. Para obter mais informações, consulte Gerar URLs pré-assinados com o S3.
- Para os casos de uso que exigem o compartilhamento de objetos do S3 entre diferentes origens, use os Pontos de Acesso S3 para criar conjuntos de permissões que restringem o acesso somente aos que estão em sua rede privada. Para obter mais informações, consulte Gerenciamento de acesso a dados com pontos de acesso do Amazon S3.
- Para conceder acesso seguro aos seus recursos do S3 para outras AWS contas, você pode usar uma lista de controle de acesso (ACL). Para obter mais informações, consulte Gerenciando o acesso ao S3 com ACLs.

Para obter mais informações sobre as opções de segurança do S3, consulte Melhores práticas de segurança do S3.

Correção de um cluster ECS potencialmente comprometido

Siga estas etapas recomendadas para corrigir um cluster Amazon ECS potencialmente comprometido em seu ambiente: AWS

1. Identifique o cluster ECS potencialmente comprometido.

   A descoberta do GuardDuty Malware Protection for ECS fornece os detalhes do cluster ECS no painel de detalhes da descoberta.

2. Avalie a origem do malware

   Verifique se o malware detectado estava na imagem do contêiner. Se a imagem contém o malware, identifique todas as outras tarefas em execução com o uso dessa imagem. Para obter informações sobre a execução de tarefas, consulte ListTasks.

3. Isole as tarefas potencialmente afetadas

   Isole as tarefas afetadas negando todo o tráfego de entrada e saída dessas tarefas. Uma regra de negar todo o tráfego pode ajudá-lo a interromper um ataque que já está em andamento, cortando todas as conexões com a tarefa.

A descoberta pode ser ignorada se o acesso foi autorizado. O console https://console.aws.amazon.com/guardduty/ permite configurar regras para suprimir totalmente as descobertas individuais e impedir sua exibição. Para ter mais informações, consulte Regras de supressão.

Correção de credenciais potencialmente comprometidas AWS

Siga estas etapas recomendadas para corrigir credenciais potencialmente comprometidas em seu ambiente: AWS

1. Identifique a entidade IAM potencialmente comprometida e a chamada de API usada.

   A chamada de API usada será listada como `API` nos detalhes da descoberta. A entidade do IAM (uma função ou usuário do IAM) e suas informações de identificação serão listadas na seção Recursos dos detalhes da descoberta. O tipo de entidade do IAM envolvida pode ser determinado pelo campo Tipo de usuário o nome da entidade do IAM estará no campo Nome de usuário. O tipo de entidade do IAM envolvida na descoberta também pode ser determinado pelo ID de chave de acesso usado.

   Para chaves que começam com `AKIA`:

   > Esse tipo de chave é uma credencial de longo prazo gerenciada pelo cliente associada a um usuário do IAM ou Usuário raiz da conta da AWS. Para obter informações sobre como gerenciar chaves de acesso para usuários do IAM, consulte Gerenciamento de chaves de acesso de usuários do IAM.

Para chaves que começam com `ASIA`:

Esse tipo de chave é uma credencial temporária de curto prazo gerada pelo AWS Security Token Service. Essas chaves existem por pouco tempo e não podem ser visualizadas nem gerenciadas no AWS Management Console. As funções do IAM sempre usarão AWS STS credenciais, mas elas também podem ser geradas para usuários do IAM. Para obter mais informações, AWS STS consulte IAM: Credenciais de segurança temporárias.

Se um perfil tiver sido usado, o campo Nome de usuário conterá informações sobre o nome do perfil usado. Você pode determinar como a chave foi solicitada AWS CloudTrail examinando o `sessionIssuer` elemento da entrada de CloudTrail registro. Para obter mais informações, consulte IAM e AWS STS informações em CloudTrail.

2. Revise as permissões para a entidade do IAM.

   Abra o console do IAM. Dependendo do tipo da entidade usada, escolha a guia Usuários ou Funções e localize a entidade afetada digitando o nome identificado no campo de pesquisa. Use as guias Permissão e Consultor de acesso para revisar permissões efetivas para essa entidade.

3. Determine se as credenciais da entidade do IAM foram usadas legitimamente.

   Entre em contato com o usuário das credenciais para determinar se a atividade foi intencional.

   Por exemplo, descubra se o usuário fez o seguinte:

   - Invocou a operação de API que foi listada na descoberta GuardDuty
   - Invocou a operação da API no horário indicado na descoberta do GuardDuty
   - Invocou a operação da API do endereço IP que foi listado na descoberta do GuardDuty

Se essa atividade for um uso legítimo das AWS credenciais, você poderá ignorar a GuardDuty descoberta. O console https://console.aws.amazon.com/guardduty/ permite configurar regras para suprimir totalmente as descobertas individuais e impedir sua exibição. Para ter mais informações, consulte Regras de supressão.

Se você não puder confirmar se essa atividade é um uso legítimo, isso pode ser o resultado de um comprometimento da chave de acesso específica: as credenciais de login do usuário do IAM ou possivelmente a totalidade. Conta da AWSSe você suspeitar que suas credenciais foram comprometidas, revise as informações no artigo Meu Conta da AWS pode estar comprometido para corrigir esse problema.

Correção de um contêiner autônomo potencialmente comprometido

1. Isole o contêiner potencialmente comprometido

   As etapas a seguir ajudarão você a identificar a carga de trabalho do contêiner potencialmente maliciosa:

   - Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
   - Na página Descobertas, escolha a descoberta correspondente para visualizar o painel de descobertas.
   - No painel de descobertas, na seção Recursos afetados, é possível ver o ID e o Nome do contêiner.

   Isole esse contêiner de outras workloads do contêiner.

2. Pause o contêiner

   Suspenda todos os processos no contêiner.

   Para obter informações sobre como congelar seu contêiner, consulte Pausar um contêiner.

   Pare o contêiner

   Se a etapa acima não funcionar e o contêiner não pausar, interrompa a execução do contêiner. Se você ativou o Retenção de snapshots recurso, GuardDuty reterá os instantâneos de seus volumes do EBS que contêm malware.

   Para obter informações sobre como parar o contêiner, consulte Parar um contêiner.

3. Avalie a presença de malware

   Verifique se o malware estava na imagem do contêiner.

A descoberta pode ser ignorada se o acesso foi autorizado. O console https://console.aws.amazon.com/guardduty/ permite configurar regras para suprimir totalmente as descobertas individuais e impedir sua exibição. O GuardDuty console permite que você configure regras para suprimir totalmente as descobertas individuais, para que elas não apareçam mais. Para ter mais informações, consulte Regras de supressão.

Como corrigir os resultados do Monitoramento de logs de auditoria do EKS

GuardDuty A Amazon gera descobertas que indicam possíveis problemas de segurança do Kubernetes quando o EKS Audit Log Monitoring está ativado em sua conta. Para ter mais informações, consulte Monitoramento de logs de auditoria do EKS. As seções a seguir descrevem as etapas de correção recomendadas para qualquer uma das situações. As ações de remediação específicas são descritas na entrada desse tipo específico de descoberta. Você pode acessar as informações completas sobre um tipo de descoberta selecionando-o na tabela Tipos de descobertas ativas.

Se algum dos tipos de descoberta do Monitoramento de logs de auditoria do EKS tiver sido gerado com expecthabilita, considere adicionar Regras de supressão para evitar futuros alertas.

Diferentes tipos de ataques e problemas de configuração podem acionar as descobertas do GuardDuty Kubernetes. Este guia ajuda você a identificar as principais causas das GuardDuty descobertas em seu cluster e descreve as diretrizes de remediação apropriadas. A seguir estão as principais causas que levaram às descobertas do GuardDuty Kubernetes:

- Possíveis problemas de configuração
- Remediando usuários potencialmente comprometidos do Kubernetes
- Corrigindo pods do Kubernetes potencialmente comprometidos
- Correção de nós Kubernetes potencialmente comprometidos
- Correção de imagens de contêineres potencialmente comprometidas

> **Note**
>
> Antes da versão 1.14 do Kubernetes, o `system:unauthenticated` grupo era associado e por padrão. `system:discovery` `system:basic-user` ClusterRoles Isso pode permitir o acesso não intencional de usuários anônimos. As atualizações de cluster não revogam essas permissões, o que significa que, mesmo que você tenha atualizado seu cluster para a versão 1.14 ou posterior, essas permissões ainda podem estar em vigor. Recomendamos que você desassocie essas permissões do grupo `system:unauthenticated`.
> Para obter mais informações sobre a remoção dessas permissões, consulte Melhores práticas de segurança para o Amazon EKS no Guia do usuário do Amazon EKS.

Possíveis problemas de configuração

Se uma descoberta indicar um problema de configuração, consulte a seção de correção dessa descoberta para obter orientação sobre como resolver esse problema específico. Para obter mais informações, consulte os tipos de descoberta a seguir que indicam problemas de configuração:

- Policy:Kubernetes/AnonymousAccessGranted
- Policy:Kubernetes/ExposedDashboard
- Policy:Kubernetes/AdminAccessToDefaultServiceAccount
- Policy:Kubernetes/KubeflowDashboardExposed
- Qualquer descoberta que termine em SuccessfulAnonymousAccess

Remediando usuários potencialmente comprometidos do Kubernetes

Uma GuardDuty descoberta pode indicar um usuário comprometido do Kubernetes quando um usuário identificado na descoberta executou uma ação inesperada da API. Você pode identificar o usuário na seção de detalhes do usuário do Kubernetes de um detalhe da descoberta no console ou no `resources.eksClusterDetails.kubernetesDetails.kubernetesUserDetails` do JSON das descobertas. Esses detalhes do usuário incluem `user name`, `uid` e os grupos do Kubernetes aos quais o usuário pertence.

Se o usuário estava acessando a workload usando uma entidade do IAM, você pode usar a seção `Access Key details` para identificar os detalhes de um usuário ou perfil do IAM. Consulte os seguintes tipos de usuário e suas diretrizes de correção.

> **Note**
>
> Você pode usar o Amazon Detective para investigar melhor o perfil do IAM ou o usuário identificado na descoberta. Ao visualizar os detalhes da descoberta no GuardDuty console, escolha Investigar em Detective. Em seguida, selecione AWS usuário ou função nos itens listados para investigá-lo em Detective.

Administrador integrado do Kubernetes: o usuário padrão atribuído pelo Amazon EKS à identidade do IAM que criou o cluster. Esse tipo de usuário é identificado pelo nome do usuário `kubernetes-admin`.

Para revogar o acesso de um administrador integrado do Kubernetes:

- Identifique o `userType` da seção `Access Key details`.
  - Se o `userType` é Perfil e o perfil pertencer a um perfil de instância do EC2:
    - Identifique essa instância e siga as instruções em Correção de uma instância potencialmente comprometida do Amazon EC2.
  - Se `userType` for Usuário ou for uma Função que foi assumida por um usuário:
    1. Gire a chave de acesso desse usuário.
    2. Alterne todos os segredos aos quais o usuário teve acesso.
    3. Revise as informações em Minha AWS conta pode estar comprometida para obter mais detalhes.

Usuário autenticado pelo OIDC: um usuário recebeu acesso por meio de um provedor do OIDC. Normalmente, um usuário do OIDC tem um endereço de e-mail como nome de usuário. Você pode verificar se o cluster usa o OIDC com o seguinte comando: `aws eks list-identity-provider-configs --cluster-name` *`your-cluster-name`*

Para revogar o acesso de um usuário autenticado pelo OIDC:

1. Alterne as credenciais desse usuário no provedor OIDC.
2. Alterne todos os segredos aos quais o usuário teve acesso.

AWS-Auth ConfigMap defined user — Um usuário do IAM que recebeu acesso por meio de um AWS-auth. ConfigMap Para obter mais informações, consulte Como gerenciar usuários ou perfis do IAM para seu cluster no guia do usuário do &EKS;. É possível revisar as permissões usando este comando: `kubectl edit configmaps aws-auth --namespace kube-system`

Para revogar o acesso de um AWS ConfigMap usuário:

1. Use o comando a seguir para abrir ConfigMap o.

```
kubectl edit configmaps aws-auth --namespace kube-system
```

2. Identifique a função ou a entrada do usuário na seção MapRoles ou MapUsers com o mesmo nome de usuário relatado na seção de detalhes do usuário do Kubernetes da sua descoberta.

GuardDuty Veja o exemplo a seguir, em que o usuário administrador foi identificado em uma descoberta.

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::444455556666:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      user name: system:node:EC2_PrivateDNSName
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::123456789012:user/admin
      username: admin
      groups:
        - system:masters
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

3. Remova esse usuário do ConfigMap. Veja o exemplo a seguir em que o usuário administrador foi removido.

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::111122223333:role/eksctl-my-cluster-nodegroup-
standard-wo-NodeInstanceRole-1WP3NUE3O6UCF
      username: system:node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:nodes
  mapUsers: |
    - userarn: arn:aws:iam::111122223333:user/ops-user
      username: ops-user
      groups:
        - system:masters
```

4. Se `userType` for Usuário ou for uma Função que foi assumida por um usuário:

   a. Gire a chave de acesso desse usuário.

b. Alterne todos os segredos aos quais o usuário teve acesso.

c. Revise as informações em Minha AWS conta pode estar comprometida para obter mais detalhes.

Se a descoberta não tiver uma seção `resource.accessKeyDetails`, o usuário é uma conta de serviço do Kubernetes.

Conta de serviço: a conta de serviço fornece uma identidade para pods e pode ser identificada por um nome de usuário com o seguinte formato: `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Para revogar o acesso a uma conta de serviço:

1. Alterne as credenciais da conta de serviço.
2. Revise a orientação sobre comprometimento de pods na seção a seguir.

Corrigindo pods do Kubernetes potencialmente comprometidos

Quando GuardDuty especifica detalhes de um pod ou recurso de carga de trabalho dentro da `resource.kubernetesDetails.kubernetesWorkloadDetails` seção, esse pod ou recurso de carga de trabalho foi potencialmente comprometido. Uma GuardDuty descoberta pode indicar que um único pod foi comprometido ou que vários pods foram comprometidos por meio de um recurso de nível superior. Consulte os seguintes cenários de comprometimento para obter orientação sobre como identificar o pod ou os pods que foram comprometidos.

Comprometimento de pods individuais

Se o campo `type` dentro da seção `resource.kubernetesDetails.kubernetesWorkloadDetails` for pods, a descoberta identifica um único pod. O campo de nome é o `name` dos pods e o campo `namespace` é seu namespace.

Para obter informações sobre como identificar o nó de trabalho que executa os pods, consulte Identificar os pods ofensivos e o nó de trabalho.

Pods comprometidos por meio de recursos de workload

Se o campo `type` dentro da seção `resource.kubernetesDetails.kubernetesWorkloadDetails` identificar um Recurso

de workload, como um `Deployment`, é provável que todos os pods desse recurso de workload tenham sido comprometidos.

Para obter informações sobre como identificar todos os pods do recurso de carga de trabalho e os nós nos quais eles estão sendo executados, consulte Identificar os pods e os nós de trabalho incorretos usando o nome da carga de trabalho.

Pods comprometidos por meio da conta de serviço

Se uma GuardDuty descoberta identificar uma conta de serviço na `resource.kubernetesDetails.kubernetesUserDetails` seção, é provável que os pods que usam a conta de serviço identificada estejam comprometidos. O nome de usuário relatado por uma descoberta é uma conta de serviço se tiver o seguinte formato: `system:serviceaccount:`*`namespace`*`:`*`service_account_name`*.

Para obter informações sobre como identificar todos os pods usando a conta de serviço e os nós nos quais eles estão sendo executados, consulte Identificar os pods e os nós de trabalho incorretos usando o nome da conta de serviço.

Depois de identificar todos os pods comprometidos e os nós nos quais eles estão sendo executados, consulte o guia de melhores práticas do Amazon EKS para isolar o pod, alternar suas credenciais e coletar dados para análise forense.

Para corrigir um pod potencialmente comprometido:

1. Identifique a vulnerabilidade que comprometeu os pods.
2. Implemente a correção para essa vulnerabilidade e inicie novos pods de substituição.
3. Exclua os pods vulneráveis.

   Para obter mais informações, consulte Reimplantar o pod comprometido ou o recurso de carga de trabalho.

Se o node de trabalho tiver recebido uma função do IAM que permite que os pods tenham acesso a outros AWS recursos, remova essas funções da instância para evitar mais danos causados pelo ataque. Da mesma forma, se o pod tiver recebido uma função do IAM, avalie se você pode remover com segurança as políticas do IAM da função sem afetar outras workloads.

Correção de imagens de contêineres potencialmente comprometidas

Quando uma GuardDuty descoberta indica um comprometimento do pod, a imagem usada para iniciar o pod pode ser potencialmente maliciosa ou estar comprometida. GuardDuty as descobertas identificam a imagem do contêiner dentro do `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.image` campo. Você pode determinar se a imagem é mal-intencionada examinando-a em busca de malware.

Para corrigir uma imagem de contêiner potencialmente comprometida:

1. Pare de usar a imagem imediatamente e remova-a do seu repositório de imagens.
2. Identifique todos os pods usando a imagem potencialmente comprometida.

   Para obter mais informações, consulte Identificar pods com imagens de contêiner e nós de trabalho potencialmente vulneráveis ou comprometidos.
3. Isole os pods potencialmente comprometidos, alterne as credenciais e colete dados para análise. Para obter mais informações, consulte o guia de melhores práticas do Amazon EKS.
4. Exclua todos os pods usando a imagem potencialmente comprometida.

Correção de nós Kubernetes potencialmente comprometidos

Uma GuardDuty descoberta pode indicar um comprometimento do nó se o usuário identificado na descoberta representar a identidade do nó ou se a descoberta indicar o uso de um contêiner privilegiado.

A identidade do usuário é um nó de processamento se o campo nome de usuário tiver o seguinte formato: `system:node:node name`. Por exemplo, `system:node:ip-192-168-3-201.ec2.internal`. Isso indica que o adversário obteve acesso ao nó e está usando as credenciais do nó para se comunicar com o endpoint da API do Kubernetes.

Uma descoberta indica o uso de um contêiner privilegiado se um ou mais dos contêineres listados na descoberta tiver o campo de descoberta `resource.kubernetesDetails.kubernetesWorkloadDetails.containers.securityContext.` definido como `True`.

Para corrigir um nó potencialmente comprometido:

1. Isole o pod, alterne suas credenciais e colete dados para análise forense.

Para obter mais informações, consulte o guia de melhores práticas do Amazon EKS.

2. Identifique as contas de serviço usadas por todos os pods em execução no nó potencialmente comprometido. Revise suas permissões e alterne as contas de serviço, se necessário.
3. Encerre o nó potencialmente comprometido.

Correção das descobertas do Runtime Monitoring

Quando você ativa o Runtime Monitoring para sua conta, a Amazon GuardDuty pode gerar informações Tipos de descoberta de monitoramento de tempo de execução que indicam possíveis problemas de segurança em seu AWS ambiente. Os possíveis problemas de segurança indicam uma instância do Amazon EC2 comprometida, carga de trabalho de contêiner, um cluster do Amazon EKS ou um conjunto de credenciais comprometidas em seu ambiente. AWS O agente de segurança monitora eventos de tempo de execução de vários tipos de recursos. Para identificar o recurso potencialmente comprometido, visualize o tipo de recurso nos detalhes da descoberta gerados no GuardDuty console. A seção a seguir descreve as etapas de correção recomendadas para qualquer tipo de recurso.

Instance

Se o tipo de recurso nos detalhes da descoberta for Instância, isso indica que uma instância do EC2 ou um nó do EKS está potencialmente comprometida.

- Para corrigir um nó EKS comprometido, consulte. Correção de nós Kubernetes potencialmente comprometidos
- Para corrigir uma instância do EC2 comprometida, consulte Correção de uma instância potencialmente comprometida do Amazon EC2.

EKSCluster

Se o Tipo de recurso nos detalhes da descoberta for EKSCluster, isso indica que um pod ou um contêiner dentro de um cluster do EKS está potencialmente comprometido.

- Para corrigir um pod comprometido, consulte. Corrigindo pods do Kubernetes potencialmente comprometidos
- Para corrigir uma imagem de contêiner comprometida, consulte. Correção de imagens de contêineres potencialmente comprometidas

ECSCluster

Se o tipo de recurso nos detalhes da descoberta for ECSCluster, isso indica que uma tarefa do ECS ou um contêiner dentro de uma tarefa do ECS está potencialmente comprometido.

1. Identifique o cluster ECS afetado

   A descoberta do GuardDuty Runtime Monitoring fornece os detalhes do cluster ECS no painel de detalhes da descoberta ou na `resource.ecsClusterDetails` seção do JSON de descoberta.

2. Identifique a tarefa afetada do ECS

   A descoberta do GuardDuty Runtime Monitoring fornece os detalhes da tarefa do ECS no painel de detalhes da descoberta ou na `resource.ecsClusterDetails.taskDetails` seção do JSON de descoberta.

3. Isole a tarefa afetada

   Isole a tarefa afetada negando todo o tráfego de entrada e saída da tarefa. Uma regra de negar todo o tráfego pode ajudar a interromper um ataque que já está em andamento, cortando todas as conexões com a tarefa.

4. Corrija a tarefa comprometida

   a. Identifique a vulnerabilidade que comprometeu a tarefa.

   b. Implemente a correção para essa vulnerabilidade e reinicie a tarefa de substituição.

   c. Pare a tarefa vulnerável.

Container

Se o tipo de recurso nos detalhes da descoberta for Contêiner, isso indica que um contêiner autônomo está potencialmente comprometido.

- Para remediar, consulte[Correção de um contêiner autônomo potencialmente comprometido](#).
- Se a descoberta for gerada em vários contêineres usando a mesma imagem de contêiner, consulte[Correção de imagens de contêineres potencialmente comprometidas](#).
- Se o contêiner acessou o host EC2 subjacente, suas credenciais de instância associadas podem ter sido comprometidas. Para obter mais informações, consulte [Correção de credenciais potencialmente comprometidas AWS](#).

- Se um ator potencialmente mal-intencionado acessou o nó EKS subjacente ou uma instância do EC2, consulte a correção recomendada nas guias EKSCluster e Instance.

Remediando imagens de contêiner comprometidas

Quando uma GuardDuty descoberta indica um comprometimento da tarefa, a imagem usada para iniciar a tarefa pode ser maliciosa ou estar comprometida. GuardDuty as descobertas identificam a imagem do contêiner dentro do `resource.ecsClusterDetails.taskDetails.containers.image` campo. Você pode determinar se a imagem é maliciosa examinando-a em busca de malware.

Para corrigir uma imagem de contêiner comprometida

1. Pare de usar a imagem imediatamente e remova-a do seu repositório de imagens.
2. Identifique todas as tarefas que estão usando essa imagem.
3. Pare todas as tarefas que estão usando a imagem comprometida. Atualize suas definições de tarefas para que parem de usar a imagem comprometida.

Corrigindo um banco de dados potencialmente comprometido

GuardDuty gerados Tipos de descoberta do RDS Protection que indicam um comportamento de login potencialmente suspeito e anômalo Bancos de dados compatíveis após a ativação. GuardDuty Proteção RDS Usando a atividade de login do RDS, GuardDuty analisa e traça perfis de ameaças identificando padrões incomuns nas tentativas de login.

> **Note**
>
> Você pode acessar as informações completas sobre um tipo de descoberta selecionando-o na Tabela de resultados.

Siga estas etapas recomendadas para corrigir um banco de dados Amazon Aurora potencialmente comprometido em seu ambiente. AWS

Tópicos

- Corrigir um banco de dados potencialmente comprometido com eventos de login bem-sucedidos
- Corrigindo um banco de dados potencialmente comprometido com eventos de login falhados

- Corrigir remediar credenciais potencialmente comprometidas
- Restringir o acesso à rede

Corrigir um banco de dados potencialmente comprometido com eventos de login bem-sucedidos

As etapas recomendadas a seguir podem ajudar você a corrigir um banco de dados Aurora potencialmente comprometido que apresenta um comportamento incomum relacionado a eventos de login bem-sucedidos.

1. Identifique o banco de dados e o usuário afetados.

   A GuardDuty descoberta gerada fornece o nome do banco de dados afetado e os detalhes do usuário correspondentes. Para ter mais informações, consulte Detalhes da descoberta.
2. Confirme se esse comportamento é esperado ou inesperado.

   A lista a seguir especifica possíveis cenários que podem ter causado GuardDuty a geração de uma descoberta:
   - Um usuário que faz login em seu banco de dados após um longo período de tempo.
   - Um usuário que faz login em seu banco de dados ocasionalmente, por exemplo, um analista financeiro que faz login a cada trimestre.
   - Um agente potencialmente suspeito envolvido em uma tentativa bem-sucedida de login pode comprometer o banco de dados.
3. Comece esta etapa se o comportamento for inesperado.

   1. Restringir acesso ao banco

      Restrinja o acesso ao banco de dados para as contas suspeitas e a origem dessa atividade de login. Para obter mais informações, consulte Restringir o acesso à rede e Corrigir remediar credenciais potencialmente comprometidas.
   2. Avalie o impacto e determine quais informações foram acessadas.
      - Se disponíveis, revise os registros de auditoria para identificar as informações que podem ter sido acessadas. Para obter mais informações, consulte Monitorar eventos, logs e streams em um cluster de banco de dados do Amazon Aurora no Guia do usuário do Amazon Aurora.
      - Determine se alguma informação confidencial ou protegida foi acessada ou modificada.

Corrigindo um banco de dados potencialmente comprometido com eventos de login falhados

As etapas recomendadas a seguir podem ajudar você a corrigir um banco de dados Aurora potencialmente comprometido que apresenta um comportamento incomum relacionado a eventos de login com falha.

1. Identifique o banco de dados e o usuário afetados.

   A GuardDuty descoberta gerada fornece o nome do banco de dados afetado e os detalhes do usuário correspondentes. Para ter mais informações, consulte Detalhes da descoberta.
2. Identifique a origem das tentativas de login malsucedidas.

   A GuardDuty descoberta gerada fornece o endereço IP e a organização ASN (se for uma conexão pública) na seção Ator do painel de descoberta.

   Um Autonomous System (AS – Sistema autônomo) é um grupo de um ou mais prefixos de IP (listas de endereços de IP acessíveis em uma rede) executados por uma ou mais operadoras de rede que mantêm uma política de roteamento única e claramente definida. As operadoras de rede precisam de Autonomous System Numbers (ASNs – Números de sistema autônomo) para controlar o roteamento em suas redes e trocar informações de roteamento com outros provedores de serviços de Internet (ISPs).
3. Confirme se esse comportamento é inesperado.

   Examine se essa atividade representa uma tentativa de obter acesso não autorizado adicional ao banco de dados da seguinte forma:
   - Se a fonte for interna, verifique se uma aplicação está configurado incorretamente e está tentando se conectar repetidamente.
   - Se for um ator externo, examine se o banco de dados correspondente está voltado para o público ou está mal configurado, permitindo que possíveis agentes mal-intencionados usem nomes de usuários comuns com força bruta.
4. Comece esta etapa se o comportamento for inesperado.

   1. Restringir acesso ao banco

      Restrinja o acesso ao banco de dados para as contas suspeitas e a origem dessa atividade de login. Para obter mais informações, consulte Restringir o acesso à rede e Corrigir remediar credenciais potencialmente comprometidas.

2. Faça uma análise da causa raiz e determine as etapas que potencialmente levaram a essa atividade.

   Configure um alerta para ser notificado quando uma atividade modifica uma política de rede e cria um estado inseguro. Para obter mais informações, consulte Políticas de firewall no AWS Network Firewall no Guia do desenvolvedor doAWS Network Firewall .

Corrigir remediar credenciais potencialmente comprometidas

Uma GuardDuty descoberta pode indicar que as credenciais do usuário de um banco de dados afetado foram comprometidas quando o usuário identificado na descoberta executou uma operação inesperada no banco de dados. Você pode identificar o usuário na seção de detalhes do usuário do RDS DB no painel de descoberta no console ou no `resource.rdsDbUserDetails` do JSON das descobertas. Esses detalhes do usuário incluem nome de usuário, aplicativo usado, banco de dados acessado, versão SSL e método de autenticação.

- Para revogar o acesso ou alternar senhas de usuários específicos envolvidos na descoberta, consulte Segurança com o Amazon Aurora MySQL ou Segurança com o Amazon Aurora PostgreSQL no Guia do usuário do Amazon Aurora.
- Use AWS Secrets Manager para armazenar com segurança e alternar automaticamente os segredos dos bancos de dados do Amazon Relational Database Service (RDS). Para obter mais informações, consulte Tutoriais doAWS Secrets Manager, no Guia do usuário doAWS Secrets Manager .
- Use a autenticação do banco de dados do IAM para gerenciar o acesso dos usuários do banco de dados sem a necessidade de senhas. Para obter mais informações, consulte Autenticação de banco de dados do IAM no Guia do usuário do Amazon Aurora.

  Para obter mais informações, consulte Práticas recomendadas de segurança do Amazon Relational Database Service no Guia do usuário do Amazon RDS.

Restringir o acesso à rede

Uma GuardDuty descoberta pode indicar que um banco de dados está acessível além de seus aplicativos ou da Virtual Private Cloud (VPC). Se o endereço IP remoto na descoberta for uma fonte de conexão inesperada, audite os grupos de segurança. Uma lista de grupos de segurança anexados ao banco de dados está disponível em Grupos de segurança no console https://

console.aws.amazon.com/rds/ ou no `resource.rdsDbInstanceDetails.dbSecurityGroups` do JSON das descobertas. Para obter mais informações sobre a configuração de grupos de segurança, consulte Controlar acesso com grupos de segurança no Guia do usuário do Amazon RDS.

Se você estiver usando um firewall, restrinja o acesso à rede ao banco de dados reconfigurando as Network Access Control Lists (NACLs – Listas de controle de acesso à rede). Para obter mais informações, consulte Firewalls no AWS Network Firewall no Guia do desenvolvedor doAWS Network Firewall .

Correção de uma função Lambda potencialmente comprometida

Quando GuardDuty gera uma descoberta do Lambda Protection e a atividade é inesperada, sua função do Lambda pode ser comprometida. Recomendamos concluir as etapas a seguir para corrigir uma função do Lambda comprometida.

Para corrigir as descobertas da Proteção do Lambda

1. Identifique a versão da função Lambda potencialmente comprometida.

   Uma GuardDuty descoberta para o Lambda Protection fornece o nome, o Amazon Resource Name (ARN), a versão da função e o ID da revisão associados à função Lambda listada nos detalhes da descoberta.
2. Identifique a origem da atividade potencialmente suspeita.

   a. Analise o código associado à versão da função do Lambda envolvida na descoberta.

   b. Analise as bibliotecas e camadas importadas da versão da função do Lambda envolvida na descoberta.

   c. Se você ativou AWS Lambda as funções de digitalização com o Amazon Inspector, revise as descobertas do Amazon Inspector associadas à função Lambda envolvida na descoberta.

   d. Analise os AWS CloudTrail registros para identificar o principal que causou a atualização da função e garantir que a atividade foi autorizada ou esperada.
3. Corrija a função Lambda potencialmente comprometida.

   a. Desabilite os acionadores de execução da função do Lambda envolvida na descoberta. Para obter mais informações, consulte DeleteFunctionEventInvokeConfig.

b. Revise o código do Lambda e atualize as importações de bibliotecas e as camadas da função do Lambda para remover as bibliotecas e camadas potencialmente suspeitas.

c. Mitigue as descobertas do Amazon Inspector relacionadas à função do Lambda envolvida na descoberta.

Gerenciando várias contas na Amazon GuardDuty

Quando seu AWS ambiente tem várias contas, você pode gerenciá-las designando uma AWS conta como sua conta de administrador. Em seguida, você pode associar outras AWS contas a essa conta de administrador como suas contas de membros. Essa conta de GuardDuty administrador designada pode configurar os planos de proteção. GuardDuty Existem duas maneiras de associar contas a uma conta de administrador: criar uma organização usando AWS Organizations e tanto a conta de administrador quanto uma ou mais contas de membros pertençam a essa organização ou enviar um convite para uma AWS conta por meio de GuardDuty.

GuardDuty recomenda o uso do AWS Organizations método. Para obter mais informações sobre como configurar uma organização, consulte Criar uma organização no Guia do usuário do AWS Organizations .

Gerenciando várias contas com AWS Organizations

Se a conta que você deseja especificar como conta de GuardDuty administrador fizer parte de uma organização AWS Organizations, você poderá especificar essa conta como administrador delegado da organização. GuardDuty A conta registrada como administrador delegado se torna automaticamente a conta do GuardDuty administrador.

Você pode usar essa conta de administrador para habilitar e gerenciar GuardDuty qualquer pessoa Conta da AWS na organização ao adicionar essa conta como conta de membro.

Se você já tem uma conta de GuardDuty administrador com contas de membros associadas por convite, você pode registrar essa conta como administrador GuardDuty delegado da organização. Ao fazer isso, todas as contas de membros atualmente associadas permanecem membros, permitindo que você aproveite ao máximo a funcionalidade adicional de gerenciar suas GuardDuty contas com AWS Organizations.

Para obter mais informações sobre o suporte a várias contas GuardDuty por meio de uma organização, consulteGerenciando GuardDuty contas com AWS Organizations.

Gerenciar várias contas por convite

Se as contas que você deseja associar não fizerem parte da sua organização, você pode especificar uma conta de administrador GuardDuty e, em seguida, usar a conta de administrador para convidar

outras pessoas Contas da AWS para se tornarem contas membros. Quando a conta convidada aceita o convite, essa conta se torna uma conta de GuardDuty membro associada à conta do administrador.

Para obter mais informações sobre como oferecer suporte a várias contas por convite, GuardDuty consulteGerenciando GuardDuty contas por convite.

Entendendo a relação entre a conta GuardDuty do administrador e as contas dos membros

Quando você usa GuardDuty em um ambiente de várias contas, a conta do administrador pode gerenciar certos aspectos GuardDuty em nome das contas dos membros. As funções principais que a conta de administrador pode executar são as seguintes:

- Adicionar e remover contas-membro associadas. O processo pelo qual isso é feito difere com base no fato de as contas estarem associadas por meio de organizações ou por convite.
- Gerencie o status das GuardDuty contas dos membros associados, incluindo a ativação e a suspensão GuardDuty.

  > **Note**
  >
  > Contas de administrador delegado gerenciadas com ativação AWS Organizations automática GuardDuty em contas adicionadas como membros.

- Personalize as descobertas na GuardDuty rede por meio da criação e gerenciamento de regras de supressão, listas de IP confiáveis e listas de ameaças. As contas-membro perdem o acesso a esses recursos em um ambiente de várias contas.

A tabela a seguir detalha a relação entre a conta GuardDuty do administrador e as contas dos membros.

Nesta tabela:

- Self — Uma conta pode realizar a ação listada somente para sua própria conta.
- Qualquer — Uma conta pode realizar a ação listada para qualquer conta associada.
- Tudo — Uma conta pode realizar a ação listada e ela se aplica a todas as contas associadas. Normalmente, a conta que executa essa ação é uma conta de GuardDuty administrador designada

As células da tabela com traço (—) indicam que a conta não pode realizar a ação listada.

Ação	Através AWS Organizations		Por convite	
	Conta de GuardDuty administrador delegada	Conta de membro associada	Conta de GuardDuty administrador delegada	Conta de membro associada
Enable GuardDuty	Any	–	Self	Self
Enable GuardDuty automatically for the entire organization (`ALL`, `NEW`, `NONE`)	All	–	–	–
View all Organizations member accounts regardless of GuardDuty status	Any	–	–	–
Generate sample findings	Self	Self	Self	Self
View all GuardDuty findings	Any	Self	Any	Self
Archive GuardDuty findings	Any	–	Any	–

Apply suppressi on rules	All	–	All	–
Create trusted IP list or threat lists	All	–	All	–
Update trusted IP list or threat lists	All	–	All	–
Delete trusted IP list or threat lists	All	–	All	–
Set EventBrid ge notification frequency	All	–	All	Self
Set Amazon S3 location for exporting findings	All	–	All	Self
Enable one or more optional protection plans for the entire organization (`ALL`, `NEW`, `NONE`)	All	–	–	–
Enable any GuardDuty protection plan for individual accounts	Any	–	Any	Self
Disassociate a member account	Any	–	Any	–

Disassociate from an administrator account account	–	Self#	–	Self
Delete a disassociated member account	Any	–	Any	–
Suspend GuardDuty	Any*	–	Any*	–
Disable GuardDuty	Any*	–	Any*	–

- # Indica que a conta pode realizar essa ação somente se a conta do GuardDuty administrador delegado não tiver configurado a preferência de ativação automática para `ALL` os membros da organização.
- * Indica que essa ação deve ser tomada para todas as contas associadas antes de ser tomada para essa conta. Depois de desassociar essas contas, você deve excluí-las. Para obter mais informações sobre como executar essas tarefas em sua organização, consulteMantendo sua organização dentro GuardDuty.

Gerenciando GuardDuty contas com AWS Organizations

Quando você usa GuardDuty com uma AWS organização, a conta de gerenciamento dessa organização pode designar qualquer conta dentro da organização como a conta de GuardDuty administrador delegado. Para essa conta de administrador, GuardDuty é ativada automaticamente somente na conta designada Região da AWS. Essa conta também tem permissão para ativar e gerenciar GuardDuty todas as contas da organização dentro dessa região. A conta do administrador pode visualizar os membros e adicionar membros a essa AWS organização.

Se você já configurou uma conta de GuardDuty administrador com contas de membros associadas por convite e as contas de membros fazem parte da mesma organização, o tipo delas muda de Por convite para Via Organizations quando você define uma conta de GuardDuty administrador delegado para sua organização. Se uma conta de GuardDuty administrador delegado adicionou

anteriormente membros por convite que não fazem parte da mesma organização, o Tipo deles permanece Por convite. Em ambos os casos, as contas adicionadas anteriormente são contas de membros associadas à conta de GuardDuty administrador delegado da organização.

É possível continuar adicionando contas como membros mesmo se elas estiverem fora da sua organização. Para obter mais informações, consulte Adicionar e gerenciar contas por convites ou Designar uma conta de GuardDuty administrador delegado e gerenciar membros usando o console GuardDuty .

Conteúdo

Considerações e recomendações ao designar uma conta de administrador delegado GuardDuty

As considerações e recomendações a seguir podem ajudá-lo a entender como uma conta de GuardDuty administrador delegado opera em: GuardDuty

Uma conta de GuardDuty administrador delegado pode gerenciar no máximo 50.000 membros.

> Há um limite de 50.000 contas de membros por conta de GuardDuty administrador delegado. Isso inclui contas de membros que foram adicionadas por meio de AWS Organizations ou aquelas que aceitaram o convite da conta de GuardDuty administrador para ingressar na organização. No entanto, pode haver mais de 50.000 contas em sua AWS organização.
>
> Se você exceder o limite de 50.000 contas de membros, receberá uma notificação e um e-mail para a conta de CloudWatch GuardDuty administrador delegado designada. AWS Health Dashboard

Uma conta de GuardDuty administrador delegado é regional.

Ao contrário AWS Organizations, GuardDuty é um serviço regional. As contas de GuardDuty administrador delegado e suas contas de membros devem ser adicionadas AWS Organizations em cada região desejada em que você GuardDuty ativou. Se a conta de gerenciamento da organização designar uma conta de GuardDuty administrador delegado somente no Leste dos EUA (Norte da Virgínia), a conta de GuardDuty administrador delegado gerenciará somente as contas de membros adicionadas à organização nessa região. Para obter mais informações sobre a paridade de recursos nas regiões onde GuardDuty está disponível, consulteRegiões e endpoints.

Casos especiais para regiões optativas

- Quando uma conta de GuardDuty administrador delegado opta por não participar de uma região opcional, mesmo que sua organização tenha a configuração de ativação GuardDuty automática definida apenas para novas contas de membros (`NEW`) ou para todas as contas de membros (`ALL`), GuardDuty não pode ser habilitada para nenhuma conta membro na organização que esteja atualmente desativada. GuardDuty Para obter informações sobre a configuração de suas contas de membros, abra Contas no painel de navegação do GuardDuty console ou use a ListMembersAPI.
- Ao trabalhar com a configuração de GuardDuty ativação automática definida como`NEW`, certifique-se de que a seguinte sequência seja atendida:

  1. As contas dos membros optam por uma região de aceitação.
  2. Adicione as contas dos membros à sua organização em AWS Organizations.

  Se você alterar a ordem dessas etapas, a configuração de GuardDuty ativação automática não **`NEW`** funcionará na região de inscrição específica porque a conta do membro não é mais nova na organização. GuardDuty fornece duas soluções alternativas:

  - Defina a configuração de GuardDuty ativação automática como`ALL`, que inclui contas de membros novas e existentes. Nesse caso, a ordem dessas etapas não é relevante.
  - Se uma conta de membro já fizer parte da sua organização, gerencie a GuardDuty configuração dessa conta individualmente na região de inscrição específica usando o GuardDuty console ou a API.

Recomendado que uma AWS organização tenha a mesma conta de GuardDuty administrador delegado em todos os Regiões da AWS.

Recomendamos que você designe a mesma conta de GuardDuty administrador delegado para sua organização em todas as áreas em Regiões da AWS que você habilitou. GuardDuty Se

você designar uma conta como conta de GuardDuty administrador delegado em uma região, é recomendável usar a mesma conta da conta de GuardDuty administrador delegado em todas as outras regiões.

Você pode designar uma nova conta de GuardDuty administrador delegado a qualquer momento. Para obter mais informações sobre como remover a conta de GuardDuty administrador delegado existente, consulteAlterando a conta do GuardDuty administrador delegado.

Não é recomendável definir a conta de gerenciamento da sua organização como a conta de GuardDuty administrador delegado.

A conta de gerenciamento da sua organização pode ser a conta de GuardDuty administrador delegado. No entanto, as práticas recomendadas de segurança da AWS seguem o princípio do privilégio mínimo e não recomendam essa configuração.

Alterar uma conta de GuardDuty administrador delegado não desativa GuardDuty as contas dos membros.

Se você remover uma conta de GuardDuty administrador delegado, GuardDuty removerá todas as contas de membros associadas a essa conta de GuardDuty administrador delegado. GuardDuty ainda permanece habilitado para todas essas contas de membros.

Permissões necessárias para designar uma conta de administrador delegado GuardDuty

Ao delegar uma conta de GuardDuty administrador delegado, você deve ter permissões para habilitar, bem GuardDuty como determinadas ações AWS Organizations da API. É possível adicionar a seguinte instrução ao final de uma política do IAM para conceder essas permissões:

```
{
    "Sid": "PermissionsForGuardDutyAdmin",
    "Effect": "Allow",
    "Action": [
        "guardduty:EnableOrganizationAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",
```

```
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
    ],
    "Resource": "*"
}
```

Além disso, se você quiser designar sua conta AWS Organizations de gerenciamento como a conta de GuardDuty administrador GuardDuty delegado, essa entidade precisará de `CreateServiceLinkedRole` permissões para inicializar. GuardDuty Para fazer isso, adicione a seguinte declaração à política do IAM e substitua *111122223333* pelo Conta da AWS ID da conta de gerenciamento da sua organização:

```
{
 "Sid": "PermissionsToEnableGuardDuty"
 "Effect": "Allow",
 "Action": [
  "iam:CreateServiceLinkedRole"
 ],
 "Resource": "arn:aws:iam::111122223333:role/aws-service-role/guardduty.amazonaws.com/
AWSServiceRoleForAmazonGuardDuty",
 "Condition": {
  "StringLike": {
   "iam:AWSServiceName": "guardduty.amazonaws.com"
  }
 }
}
```

Designar uma conta de GuardDuty administrador delegado e gerenciar membros usando o console GuardDuty

Conteúdo

Etapa 1 — Designar uma conta de GuardDuty administrador delegado para sua organização

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Para fazer login, use as credenciais da conta de gerenciamento de sua organização da AWS Organizations .
2. Se você já ativou GuardDuty a conta de gerenciamento, pule esta etapa e siga a próxima etapa.

   Se você GuardDuty ainda não ativou, selecione Começar e, em seguida, designe uma conta de GuardDuty administrador delegado na página Bem-vindo ao GuardDuty.

   > **Note**
   >
   > A conta de gerenciamento deve ter a função GuardDuty vinculada ao serviço (SLR) para que a conta do GuardDuty administrador delegado possa ser ativada e GuardDuty gerenciada nessa conta. Depois de habilitar GuardDuty em uma região para a conta de gerenciamento, essa SLR é criada automaticamente.
3. Execute essa etapa depois de habilitar GuardDuty a conta de gerenciamento. No painel de navegação do GuardDuty console, escolha Configurações. Na página Configurações, insira o Conta da AWS ID de 12 dígitos da conta que você deseja designar como a conta de GuardDuty administrador delegado da organização.

   Certifique-se de habilitar sua conta GuardDuty de GuardDuty administrador delegado recém-designada, caso contrário, ela não poderá realizar nenhuma ação.
4. Escolha Delegar.
5. (Recomendado) Repita a etapa anterior para designar a conta de GuardDuty administrador delegado em cada uma das áreas em Região da AWS que você GuardDuty ativou.

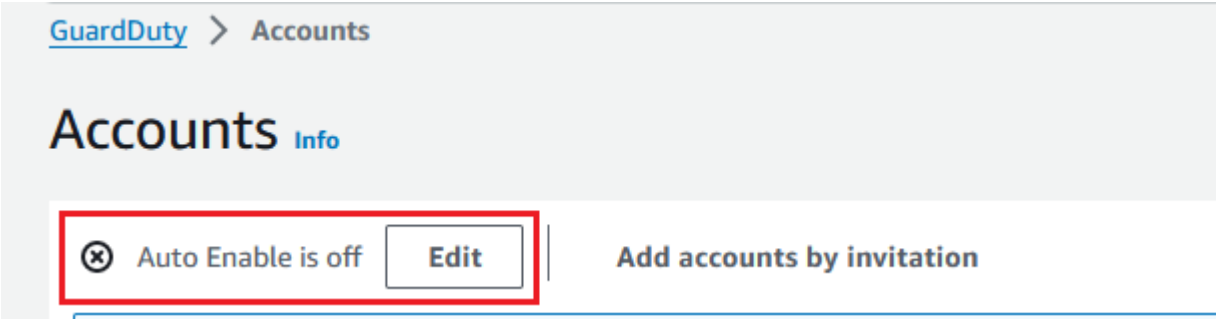
Etapa 2 — Configurando as preferências de ativação automática para sua organização

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Para entrar, use as credenciais da conta de GuardDuty administrador.
2. No painel de navegação, escolha Accounts (Contas).

A página Contas fornece opções de configuração para a conta do GuardDuty administrador ser ativada automaticamente GuardDuty e os planos de proteção opcionais em nome das contas membros que pertencem à organização.

3. Para atualizar as configurações de ativação automática existentes, escolha Editar.



Esse suporte está disponível para configuração GuardDuty e para todos os planos de proteção opcionais compatíveis em seu Região da AWS. Você pode selecionar uma das seguintes opções de configuração GuardDuty em nome de suas contas de membros:

- Ativar para todas as contas (**`ALL`**) — Selecione para ativar a opção correspondente para todas as contas em uma organização. Isso inclui novas contas que ingressam na organização e aquelas contas que podem ter sido suspensas ou removidas da organização. Isso também inclui a conta de GuardDuty administrador delegado.

  > **Note**
  >
  > Pode levar até 24 horas para atualizar a configuração de todas as contas dos membros.

- Ativação automática para novas contas (**`NEW`**) — Selecione para ativar GuardDuty ou ativar os planos de proteção opcionais somente para novas contas de membros automaticamente quando elas ingressarem na sua organização.
- Não habilitar (**`NONE`**) — Selecione para evitar a ativação da opção correspondente para novas contas em sua organização. Nesse caso, a conta GuardDuty do administrador gerenciará cada conta individualmente.

  Quando você atualiza a configuração de ativação automática de `ALL` ou `NEW` para`NONE`, essa ação não desativa a opção correspondente para suas contas existentes. Essa configuração se aplicará às novas contas que ingressarem na organização. Depois de atualizar as

configurações de ativação automática, nenhuma nova conta terá a opção correspondente ativada.

> **Note**
>
> Quando uma conta de GuardDuty administrador delegado opta por não participar de uma região opcional, mesmo que sua organização tenha a configuração de ativação GuardDuty automática definida apenas para novas contas de membros (`NEW`) ou para todas as contas de membros (`ALL`), GuardDuty não pode ser habilitada para nenhuma conta membro na organização que esteja atualmente desativada. GuardDuty Para obter informações sobre a configuração de suas contas de membros, abra Contas no painel de navegação do GuardDuty console ou use a ListMembersAPI.

4. Escolha Salvar alterações.
5. (Opcional) se você quiser usar as mesmas preferências em cada região, atualize suas preferências em cada uma das regiões suportadas separadamente.

   Alguns dos planos de proteção opcionais podem não estar disponíveis em todos os Regiões da AWS lugares GuardDuty disponíveis. Para ter mais informações, consulte Regiões e endpoints.

Etapa 3: adicionar contas como membros da organização

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Para fazer login, use as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, escolha Accounts (Contas).

   A tabela de contas exibe todas as contas que são adicionadas Via Organizations (AWS Organizations) ou Por convite. Se uma conta de membro não estiver associada à conta de GuardDuty administrador da organização, o status dessa conta de membro será Não membro.
3. Selecione um ou vários IDs de conta que você deseja adicionar como membros. Esses IDs de conta devem ter o Tipo de Via Organizations.

   As contas adicionadas por meio de convite não fazem parte da sua organização. Você pode gerenciar essas contas individualmente. Para ter mais informações, consulte Gerenciando contas por convite.

4. Escolha o menu suspenso Ações e escolha Adicionar membro. Depois de adicionar essa conta como membro, a GuardDuty configuração de ativação automática será aplicada. Com base nas configurações emthe section called “Etapa 1 — Designar uma conta de GuardDuty administrador delegado para sua organização”, a GuardDuty configuração dessas contas pode mudar.
5. Você pode selecionar a seta para baixo da coluna Status para classificar as contas pelo status Não é membro e, em seguida, escolher cada conta que não GuardDuty esteja ativada na região atual.

   Se nenhuma das contas listadas na tabela de contas ainda tiver sido adicionada como membro, você poderá habilitar GuardDuty na região atual todas as contas da organização. Escolha a opção para habilitar na faixa na parte superior da página. Essa ação ativa automaticamente a GuardDuty configuração de ativação automática para que seja GuardDuty habilitada para qualquer nova conta que ingresse na organização.
6. Selecione Confirmar para adicionar as contas como membros. Essa ação também é GuardDuty ativada para todas as contas selecionadas. O Status das contas convidadas será alterado para Habilitado.
7. (Recomendado) Repita essas etapas em cada uma Região da AWS. Isso garante que a conta de GuardDuty administrador delegado possa gerenciar descobertas e outras configurações para contas de membros em todas as regiões em que GuardDuty você habilitou.

   O recurso de ativação automática habilita todos GuardDuty os futuros membros de sua organização. Isso permite que sua conta de GuardDuty administrador delegado gerencie quaisquer novos membros criados ou adicionados à organização. Quando o número de contas de membros atinge o limite de 50.000, o recurso de ativação automática é desativado automaticamente. Se você remover uma conta de membro e o número total de membros diminuir para menos de 50.000, o recurso de ativação automática será ativado novamente.

(Opcional) etapa 4 — Configurar planos de proteção para contas individuais

Você pode configurar planos de proteção para contas individuais na página Contas.

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Use as credenciais da conta de GuardDuty administrador delegado.
2. No painel de navegação, escolha Accounts (Contas).
3. Selecione uma ou mais contas para as quais você deseja configurar um plano de proteção. Repita as etapas a seguir para cada plano de proteção que você deseja configurar:

a. Selecione Editar planos de proteção.

b. Na lista de planos de proteção, escolha um plano de proteção que deseja configurar.

c. Selecione uma das ações que você deseja realizar para esse plano de proteção e, em seguida, selecione Confirmar.

d. Para a conta selecionada, a coluna correspondente ao plano de proteção configurado mostrará a configuração atualizada como Habilitada ou Não habilitada.

Designar uma conta de GuardDuty administrador GuardDuty delegado e gerenciar membros usando a API

Conteúdo

Etapa 1 — Designar uma conta de GuardDuty administrador delegado para sua organização AWS

1. Execute enableOrganizationAdminAccountusando as credenciais da conta Conta da AWS de gerenciamento da organização.

   - Como alternativa, você pode usar AWS Command Line Interface para fazer isso. O AWS CLI comando a seguir designa uma conta de GuardDuty administrador delegado somente para sua região atual. Execute o AWS CLI comando a seguir e certifique-se de substituir *111111111111* pela Conta da AWS ID da conta que você deseja designar como conta de administrador delegado: GuardDuty

     ```
     aws guardduty enable-organization-admin-account --admin-account-id 111111111111
     ```

     Para designar a conta de GuardDuty administrador delegado para outras regiões, especifique a região no AWS CLI comando. O exemplo a seguir demonstra como habilitar uma conta de GuardDuty administrador delegado no Oeste dos EUA (Oregon). Certifique-se de substituir *us-west-2* pela região à qual você deseja atribuir a conta de administrador GuardDuty delegado GuardDuty .

```
aws guardduty enable-organization-admin-account --admin-account-id 111111111111
 --region us-west-2
```

Para obter informações sobre Regiões da AWS onde GuardDuty está disponível, consulteRegiões e endpoints.

Se não GuardDuty estiver habilitado para sua conta de GuardDuty administrador delegado, não será possível realizar nenhuma ação. Se ainda não tiver feito isso, certifique-se de habilitar a conta GuardDuty de GuardDuty administrador delegado recém-designada.

2. (Recomendado) repita a etapa anterior para designar a conta de GuardDuty administrador delegado em cada uma das áreas em Região da AWS que você GuardDuty ativou.

Etapa 2: configurar as preferências de habilitação automática para a organização

1. 1. Execute UpdateOrganizationConfigurationusando as credenciais da conta de GuardDuty administrador delegado, para configurar automaticamente planos GuardDuty de proteção opcionais nessa região para sua organização

   Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

   > **Note**
   >
   > Para obter informações sobre as várias configurações de ativação automática, consulte autoEnableOrganization Membros.

   2. Para definir preferências de habilitação automática para qualquer um dos planos de proteção opcionais compatíveis em sua região, siga as etapas fornecidas nas seções de documentação correspondentes de cada plano de proteção.
   3. Você pode validar as preferências da sua organização na região atual. Executar describeOrganizationConfiguration. Certifique-se de especificar o ID do detector da conta do GuardDuty administrador delegado.

   > **Note**
   >
   > Pode levar até 24 horas para atualizar a configuração de todas as contas-membro.

- 1. Como alternativa, execute o AWS CLI comando a seguir para definir as preferências a serem ativadas ou desativadas automaticamente GuardDuty nessa região para novas contas (`NEW`) que ingressam na organização, todas as contas (`ALL`) ou nenhuma das contas (`NONE`) na organização. Para obter mais informações, consulte autoEnableOrganizationMembros. Com base na sua preferência, talvez seja necessário substituir `NEW` por `ALL` ou `NONE`. Se você configurar o plano de proteção com`ALL`, o plano de proteção também será habilitado para a conta de GuardDuty administrador delegado. Certifique-se de especificar o ID do detector da conta do GuardDuty administrador delegado que gerencia a configuração da organização.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty update-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0 --auto-enable-organization-members=NEW
  ```

  2. Você pode validar as preferências da sua organização na região atual. Execute o AWS CLI comando a seguir usando o ID do detector da conta do GuardDuty administrador delegado.

  ```
  aws guardduty describe-organization-configuration --detector-
  id 12abc34d567e8fa901bc2d34e56789f0
  ```

2. (Recomendado) repita as etapas anteriores em cada região usando o ID delegado do detector da conta de GuardDuty administrador.

> **Note**
>
> Quando uma conta de GuardDuty administrador delegado opta por não participar de uma região opcional, mesmo que sua organização tenha a configuração de ativação GuardDuty automática definida apenas para novas contas de membros (`NEW`) ou para todas as contas de membros (`ALL`), GuardDuty não pode ser habilitada para nenhuma conta membro na organização que esteja atualmente desativada. GuardDuty Para obter informações sobre a configuração de suas contas de membros, abra Contas no painel de navegação do GuardDuty console ou use a ListMembersAPI.

Etapa 3: adicionar contas como membros da organização

- Execute CreateMembersusando as credenciais da conta de GuardDuty administrador delegado designada na etapa anterior.

  Você deve especificar o ID do detector regional da conta do GuardDuty administrador delegado e os detalhes da conta (Conta da AWS IDs e endereços de e-mail correspondentes) das contas que você deseja adicionar como GuardDuty membros. É possível criar um ou mais membros com essa operação de API.

  Quando você trabalha CreateMembers em sua organização, as preferências de ativação automática para novos membros serão aplicadas à medida que novas contas de membros ingressarem na sua organização. Quando você executa CreateMembers com uma conta de membro existente, a configuração da organização também se aplica aos membros existentes. Isso pode alterar a configuração atual das contas de membros existentes.

  Execute ListAccountsna Referência AWS Organizations da API para ver todas as contas na AWS organização.

  > **Important**
  >
  > Quando você adiciona uma conta como GuardDuty membro, ela será GuardDuty ativada automaticamente nessa região. Há uma exceção na conta de gerenciamento da organização. Antes que a conta de gerenciamento seja adicionada como GuardDuty membro, ela deve estar GuardDuty ativada.

- Como alternativa, você pode usar AWS Command Line Interface. Execute o comando AWS CLI a seguir e certifique-se de usar seu próprio ID de detector válido, ID de Conta da AWS e endereço de e-mail associado ao ID da conta.

  Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

  ```
  aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
  account-details AccountId=111122223333,Email=guardduty-member-name@amazon.com
  ```

Você pode ver uma lista de todos os membros da organização executando o seguinte AWS CLI comando:

```
aws organizations list-accounts
```

Depois de adicionar essa conta como membro, a GuardDuty configuração de ativação automática será aplicada.

Mantendo sua organização dentro GuardDuty

Como conta de GuardDuty administrador delegado, você é responsável por manter a configuração GuardDuty e seus planos de proteção opcionais para todas as contas da sua organização em cada uma das contas suportadas Região da AWS. As seções a seguir fornecem as opções para manter o status da configuração GuardDuty ou de qualquer um de seus planos de proteção opcionais:

Para manter o status de configuração de toda a sua organização em cada região

- Defina preferências de ativação automática para toda a organização usando o GuardDuty console — Você pode habilitar GuardDuty automaticamente para todos (`ALL`) os membros da organização ou novos (`NEW`) membros que ingressam na organização, ou optar por não (`NONE`) ativá-la automaticamente para nenhum dos membros da organização.

  Você também pode definir configurações iguais ou diferentes para qualquer um dos planos de proteção incluídos GuardDuty.

  Pode levar até 24 horas para atualizar a configuração de todas as contas dos membros na organização.
- Atualize as preferências de ativação automática usando a API — Execute UpdateOrganizationConfigurationpara configurar automaticamente GuardDuty e seus planos de proteção opcionais para a organização. Quando você corre CreateMemberspara adicionar novas contas de membros em sua organização, as configurações definidas serão aplicadas automaticamente. Quando você executa CreateMembers com uma conta de membro existente, a configuração da organização também se aplica aos membros existentes. Isso pode alterar a configuração atual das contas de membros existentes.

  Para ver todas as contas em sua organização, execute ListAccountsna Referência da AWS Organizations API.

Para manter o status de configuração das contas dos membros individualmente em cada região

- Para ver todas as contas em sua organização, execute ListAccountsna Referência da AWS Organizations API.
- Quando você quiser que contas de membros seletivas tenham um status de configuração diferente, execute UpdateMemberDetectorspara cada conta de membro individualmente.

  Você pode usar o GuardDuty console para realizar a mesma tarefa navegando até a página Contas no GuardDuty console.

  Para obter informações sobre como habilitar planos de proteção para contas individuais usando o console ou a API, consulte a página de configuração do plano de proteção correspondente.

Alterando a conta do GuardDuty administrador delegado

Você pode alterar a conta de GuardDuty administrador delegado da sua organização em cada região e, em seguida, delegar um novo administrador em cada região. Para manter uma postura de segurança para as contas dos membros da sua organização em uma região, você deve ter uma conta de GuardDuty administrador delegada nessa região.

Removendo a conta de GuardDuty administrador delegado existente

Etapa 1 - Para remover a conta de GuardDuty administrador delegado existente em cada região

1. Como conta de GuardDuty administrador delegado existente, liste todas as contas de membros associadas à sua conta de administrador. Corra ListMemberscom`OnlyAssociated=false`.
2. Se a preferência de ativação automática GuardDuty ou qualquer um dos planos de proteção opcionais estiver definida como`ALL`, execute UpdateOrganizationConfigurationpara atualizar a configuração da organização para `NEW` ou`NONE`. Essa ação evitará um erro ao desassociar todas as contas dos membros na próxima etapa.
3. Execute DisassociateMemberspara desassociar todas as contas de membros associadas à conta de administrador.
4. Execute DeleteMemberspara excluir as associações entre a conta do administrador e as contas dos membros.
5. Como conta de gerenciamento da organização, execute DisableOrganizationAdminAccountpara remover a conta de GuardDuty administrador delegado existente.

6. Repita essas etapas em cada um Região da AWS em que você tenha essa conta de GuardDuty administrador delegado.

Etapa 2 - Para cancelar o registro da conta de GuardDuty administrador delegado existente em AWS Organizations (ação global única)

- Execute DeregisterDelegatedAdministratorna Referência da AWS Organizations API para cancelar o registro da conta de GuardDuty administrador delegado existente em. AWS Organizations

  Como alternativa, você pode executar o seguinte AWS CLI comando:

  ```
  aws organizations deregister-delegated-administrator --account-id 111122223333 --
  service-principal guardduty.amazonaws.com
  ```

  Certifique-se de substituir *111122223333* pela conta de administrador delegado existente. GuardDuty

  Depois de cancelar o registro da antiga conta de GuardDuty administrador delegado, você pode adicioná-la como uma conta de membro à nova conta de administrador delegado GuardDuty .

Designação de uma nova conta de GuardDuty administrador delegado em cada região

1. Designe uma nova conta de GuardDuty administrador delegado em cada região usando um dos seguintes métodos de acesso:

   - Usando o GuardDuty console —Etapa 1 — Designar uma conta de GuardDuty administrador delegado para sua organização.
   - Usando GuardDuty API —Etapa 1 — Designar uma conta de GuardDuty administrador delegado para sua organização AWS.
2. Execute DescribeOrganizationConfigurationpara ver a configuração atual de ativação automática da sua organização.

   > **Important**
   >
   > Antes de adicionar qualquer membro à nova conta de GuardDuty administrador delegado, você deve verificar a configuração de ativação automática da sua

organização. Essa configuração é específica para a nova conta de GuardDuty administrador delegado e para a região selecionada e não está relacionada a. AWS Organizations Quando você adiciona uma conta de membro da organização (nova ou existente) à nova conta de GuardDuty administrador delegado, a configuração de ativação automática da nova conta de GuardDuty administrador delegado será aplicada no momento da ativação GuardDuty ou de qualquer um de seus planos de proteção opcionais.

Para alterar essa configuração da organização para a nova conta de GuardDuty administrador delegado, use um dos seguintes métodos de acesso:

- Usando o GuardDuty console —Etapa 2 — Configurando as preferências de ativação automática para sua organização.
- Usando GuardDuty API —Etapa 2: configurar as preferências de habilitação automática para a organização.

Gerenciando GuardDuty contas por convite

Para gerenciar contas fora da organização, é possível usar o método de convite legado. Ao usar esse método, sua conta é designada como uma conta de administrador quando outra conta aceita seu convite para se tornar uma conta-membro.

Se sua conta não for uma conta de administrador, você poderá aceitar um convite de outra conta. Quando você aceitar, sua conta se tornará uma conta-membro. Uma AWS conta não pode ser uma conta de GuardDuty administrador e uma conta de membro ao mesmo tempo.

Ao aceitar um convite de uma conta, você não pode aceitar um convite de outra conta. Para aceitar um convite de outra conta, primeiro você precisará desassociar sua conta da conta de administrador existente. Como alternativa, a conta do administrador também pode desassociar e remover sua conta da organização.

As contas associadas por convite têm o mesmo account-to-member relacionamento geral de administrador que as contas associadas por AWS Organizations, conforme descrito emEntendendo a relação entre a conta GuardDuty do administrador e as contas dos membros. No entanto, os usuários da conta de administrador de convites não podem ativar GuardDuty contas de membros associadas ou visualizar outras contas de não membros em sua AWS Organizations organização.

> **Important**
>
> A transferência de dados entre regiões pode ocorrer ao GuardDuty criar contas de membros usando esse método. Para verificar os endereços de e-mail das contas dos membros, GuardDuty usa um serviço de verificação de e-mail que opera somente na região Leste dos EUA (Norte da Virgínia).

Adicionar e gerenciar contas por convites

Escolha um dos métodos de acesso para adicionar e convidar contas para se tornarem contas de GuardDuty membros como conta de GuardDuty administrador.

Console

Etapa 1 – Adicionar uma conta

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Accounts (Contas).
3. Escolha Add accounts by invitation (Adicionar contas por convite) no painel superior.
4. Na página Adicionar contas de membros, em Inserir detalhes da conta, insira o Conta da AWS ID e o endereço de e-mail associados à conta que você deseja adicionar.
5. Para adicionar outra linha para inserir os detalhes da conta, um por vez, escolha Adicionar outra conta. Você também pode escolher Carregar arquivo.csv com detalhes da conta para adicionar contas em massa.

   > **Important**
   >
   > A primeira linha do arquivo .csv deve conter o cabeçalho, como ilustrado no exemplo a seguir: `Account ID,Email`. Cada linha subsequente deve conter uma única Conta da AWS ID válida e o endereço de e-mail associado. O formato de uma linha é válido se ela contiver somente uma Conta da AWS ID e o endereço de e-mail associado separados por uma vírgula.

   ```
   Account ID,Email
   555555555555,user@example.com
   ```

6. Depois de adicionar todos os detalhes das contas, escolha Próximo. Você pode ver as contas recém-adicionadas na tabela Contas. O status dessas contas será Convite não enviado. Para obter informações sobre como enviar um convite para uma ou mais contas adicionadas, consulte Step 2 - Invite an account.

Etapa 2 – Convidar uma conta

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, escolha Accounts (Contas).
3. Selecione uma ou mais contas que você deseja convidar para a Amazon GuardDuty.
4. Selecione o menu suspenso Ações e, em seguida, selecione Convidar.
5. Na caixa de GuardDuty diálogo Convite para, insira uma mensagem de convite (opcional).

   Se a conta convidada não tiver acesso a e-mail, marque a caixa de seleção Enviar também uma notificação por e-mail para o usuário raiz na Conta da AWS do convidado e gerar um alerta no AWS Health Dashboard do convidado.
6. Selecione Send invitation (Enviar convite). Se os convidados tiverem acesso ao endereço de e-mail especificado, eles poderão ver o convite abrindo o GuardDuty console em https://console.aws.amazon.com/guardduty/.
7. Quando um convidado aceita o convite, o valor na coluna Status muda para Convidado. Para obter informações sobre como gerenciar um convite, consulte Step 3 - Accept an invitation.

Etapa 3 – Aceitar um convite

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   > **Important**
   >
   > Você deve habilitar GuardDuty antes de poder ver ou aceitar um convite de associação.

2. Faça o seguinte somente se você GuardDuty ainda não tiver ativado; caso contrário, você pode pular essa etapa e continuar com a próxima etapa.

   Se você ainda não habilitou GuardDuty, escolha Get Started na GuardDuty página da Amazon.

Na GuardDuty página Bem-vindo ao, escolha Ativar GuardDuty.

3. Depois de ativar GuardDuty sua conta, use as etapas a seguir para aceitar o convite de associação:

   a. No painel de navegação, selecione Configurações.

   b. Escolha Accounts.

   c. Em Contas, certifique-se de verificar o proprietário da conta da qual você aceita o convite. Habilite a opção Aceitar para aceitar o convite de membro.

4. Depois de aceitar o convite, sua conta se torna uma conta de GuardDuty membro. A conta cujo proprietário enviou o convite se torna a conta GuardDuty do administrador. A conta do administrador saberá que você aceitou o convite. A tabela de contas em sua GuardDuty conta será atualizada. O valor na coluna Status correspondente ao ID da sua conta de membro será alterado para Ativado. O proprietário da conta de administrador agora pode visualizar GuardDuty e gerenciar as configurações do plano de proteção em nome da sua conta. A conta do administrador também pode visualizar e gerenciar GuardDuty as descobertas geradas para sua conta de membro.

API/CLI

Você pode designar uma conta de GuardDuty administrador e criar ou adicionar contas de GuardDuty membros por convite por meio das operações da API. Execute as seguintes operações de GuardDuty API para designar contas de administrador e contas de membros em GuardDuty.

Conclua o procedimento a seguir usando as credenciais da Conta da AWS que você deseja designar como conta de GuardDuty administrador.

Criação ou adição de contas-membro

1. Execute a operação da CreateMembersAPI usando as credenciais da AWS conta que foi GuardDuty ativada. Essa é a conta que você deseja que seja a GuardDuty conta de administrador.

   Você deve especificar o ID do detector da AWS conta atual e o ID da conta e o endereço de e-mail das contas das quais você deseja que se tornem GuardDuty membros. É possível criar um ou mais membros com essa operação de API.

Você também pode usar as ferramentas de linha de AWS comando para designar uma conta de administrador executando o seguinte comando da CLI. Use seu próprio ID de detector válido, ID da conta e e-mail.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

```
aws guardduty create-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
account-details AccountId=111122223333,Email=guardduty-member@organization.com
```

2. Execute InviteMembersusando as credenciais da AWS conta que foi GuardDuty ativada. Essa é a conta que você deseja que seja a GuardDuty conta de administrador.

   Você deve especificar o ID do detector da AWS conta atual e os IDs das contas das quais você deseja que se tornem GuardDuty membros. Você pode convidar um ou mais membros com essa operação de API.

   > **Note**
   >
   > Você também pode especificar uma mensagem de convite opcional usando o parâmetro de solicitação `message`.

   Você também pode usar AWS Command Line Interface para designar contas de membros executando o comando a seguir. Use seu próprio ID de detector e IDs válidos das contas que você deseja convidar.

   Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

   ```
   aws guardduty invite-members --detector-id 12abc34d567e8fa901bc2d34e56789f0 --
   account-ids 111122223333
   ```

Como aceitar convites

Conclua o procedimento a seguir usando as credenciais de cada AWS conta que você deseja designar como conta de GuardDuty membro.

1. Execute a operação da CreateDetectorAPI para cada AWS conta que foi convidada para se tornar uma conta GuardDuty membro e que você deseja aceitar um convite.

   Você deve especificar se o recurso do detector deve ser ativado usando o GuardDuty serviço. Um detector deve ser criado e ativado para que ele GuardDuty se torne operacional. Você deve primeiro habilitar GuardDuty antes de aceitar um convite.

   Você também pode fazer isso usando as ferramentas de linha de AWS comando usando o seguinte comando da CLI.

   ```
   aws guardduty create-detector --enable
   ```

2. Execute a operação da AcceptAdministratorInvitationAPI para cada AWS conta em que você deseja aceitar o convite de associação, usando as credenciais dessa conta.

   Você deve especificar o ID do detector dessa AWS conta para a conta do membro, o ID da conta do administrador que enviou o convite e o ID do convite que você está aceitando. É possível encontrar o ID da conta de administrador no e-mail de convite ou usando a operação de API ListInvitations.

   Você também pode aceitar um convite usando as ferramentas de linha de AWS comando executando o seguinte comando da CLI. Use um ID de detector válido, o ID da conta de administrador e ID de convite.

   Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

   ```
   aws guardduty accept-invitation --detector-id 12abc34d567e8fa901bc2d34e56789f0
    --administrator-id 444455556666 --invitation-
   id 84b097800250d17d1872b34c4daadcf5
   ```

Consolidação de contas de GuardDuty administrador em uma única conta de administrador delegado GuardDuty da organização

GuardDuty recomenda usar a associação AWS Organizations para gerenciar contas de membros em uma conta de GuardDuty administrador delegado. Você pode usar o processo de exemplo descrito abaixo para consolidar a conta de administrador e o membro associado por convite em uma organização em uma única conta de administrador GuardDuty delegado GuardDuty .

> **Note**
>
> Contas que já estão sendo gerenciadas por uma conta de GuardDuty administrador delegado ou contas de membros ativas associadas à conta de GuardDuty administrador delegado não podem ser adicionadas a uma conta de administrador delegado GuardDuty diferente. Cada organização pode ter somente uma conta de GuardDuty administrador delegado por região, e cada conta de membro pode ter somente uma conta de GuardDuty administrador delegado.

Escolha um dos métodos de acesso para consolidar contas de GuardDuty administrador em uma única conta de GuardDuty administrador delegado.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Para fazer login, use as credenciais da conta de gerenciamento da organização.
2. Todas as contas que você deseja gerenciar GuardDuty devem fazer parte da sua organização. Para obter informações sobre como adicionar uma conta à sua organização, consulte Convidar um Conta da AWS para participar da sua organização.
3. Verifique se todas as contas dos membros estão associadas à conta que você deseja designar como a única conta de GuardDuty administrador delegado. Desassocie qualquer conta de membro que ainda esteja associada às contas de administrador preexistentes.

   As etapas a seguir ajudarão você a desassociar contas-membro da conta de administrador preexistente:

   a. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
   b. Para fazer login, use as credenciais da conta de administrador preexistente.
   c. No painel de navegação, escolha Accounts (Contas).
   d. Na página Contas, selecione uma ou mais contas que você deseja desassociar da conta de administrador.
   e. Selecione Ações e, em seguida, selecione Desassociar conta.
   f. Selecione Confirmar para finalizar a etapa.
4. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

Para fazer login, use as credenciais da conta de gerenciamento.

5. No painel de navegação, selecione Configurações. Na página Configurações, designe a conta de GuardDuty administrador delegado para a organização.
6. Faça login na conta de GuardDuty administrador delegado designada.
7. Adicione membros da organização. Para ter mais informações, consulte Gerenciando GuardDuty contas com AWS Organizations.

API/CLI

1. Todas as contas que você deseja gerenciar GuardDuty devem fazer parte da sua organização. Para obter informações sobre como adicionar uma conta à sua organização, consulte Convidar um Conta da AWS para participar da sua organização.
2. Verifique se todas as contas dos membros estão associadas à conta que você deseja designar como a única conta de GuardDuty administrador delegado.

   a. Execute DisassociateMemberspara desassociar qualquer conta de membro que ainda esteja associada às contas de administrador preexistentes.

   b. Como alternativa, você pode usar AWS Command Line Interface para executar o comando a seguir e substituir *7777777777* pelo ID do detector da conta de administrador preexistente da qual você deseja desassociar a conta do membro. Substitua *666666666666* pelo ID da Conta da AWS do membro que você deseja desassociar.

   ```
   aws guardduty disassociate-members --detector-id 777777777777 --account-
   ids 666666666666
   ```

3. Execute EnableOrganizationAdminAccountpara delegar uma Conta da AWS como conta de GuardDuty administrador delegado.

   Como alternativa, você pode usar AWS Command Line Interface para executar o seguinte comando para delegar uma conta de GuardDuty administrador delegado:

   ```
   aws guardduty enable-organization-admin-account --admin-account-id 777777777777
   ```

4. Adicione membros da organização. Para ter mais informações, consulte Create or add member member accounts using API.

> **Important**
>
> Para maximizar a eficácia de GuardDuty um serviço regional, recomendamos que você designe sua conta de GuardDuty administrador delegado e adicione todas as suas contas de membros em cada região.

Habilite GuardDuty em várias contas simultaneamente

Use o método a seguir para habilitar GuardDuty em várias contas ao mesmo tempo.

Use scripts Python para habilitar várias GuardDuty contas simultaneamente

Você pode automatizar a ativação ou desativação de GuardDuty em várias contas usando os scripts do repositório de amostras nos scripts multicontas da Amazon GuardDuty . Use o processo nesta seção GuardDuty para habilitar uma lista de contas de membros usando o Amazon EC2. Para obter informações sobre como usar o script de desativação ou configurar o script localmente, consulte as instruções no link compartilhado.

O `enableguardduty.py` script ativa GuardDuty, envia convites da conta do administrador e aceita convites em todas as contas dos membros. O resultado é uma GuardDuty conta de administrador que contém todas as descobertas de segurança de todas as contas de membros. Como GuardDuty é isolado por região, as descobertas de cada conta de membro são acumuladas na região correspondente na conta do administrador. Por exemplo, a região us-east-1 em sua conta de GuardDuty administrador contém as descobertas de segurança de todas as descobertas us-east-1 de todas as contas de membros associadas.

Esses scripts dependem de uma função compartilhada do IAM com a política gerenciada – AWS política gerenciada: AmazonGuardDutyFullAccess. Essa política fornece às entidades acesso GuardDuty e deve estar presente na conta do administrador e em cada conta para a qual você deseja habilitar GuardDuty.

O processo a seguir é ativado GuardDuty em todas as regiões disponíveis por padrão. Você pode habilitar GuardDuty em regiões especificadas somente usando o `--enabled_regions` argumento opcional e fornecendo uma lista de regiões separadas por vírgulas. Você também pode personalizar a mensagem de convite enviada para contas-membro abrindo o `enableguardduty.py` e editando a string `gd_invite_message`.

1. Crie uma função do IAM na conta do GuardDuty administrador e anexe a AWS política gerenciada: AmazonGuardDutyFullAccess política para habilitá-la GuardDuty.
2. Crie uma função do IAM em cada conta de membro que você deseja que seja gerenciada pela sua conta de GuardDuty administrador. Essa função deve ter o mesmo nome da função criada na etapa 1, deve permitir a conta do administrador como uma entidade confiável e deve ter a mesma política AmazonGuardDutyFullAccess gerenciada descrita anteriormente.
3. Execute uma nova instância do Amazon Linux com uma função associada que tenha a relação de confiança a seguir que permita à instância assumir uma função de serviço.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Faça login na nova instância e execute os comandos a seguir para configurá-la.

```
sudo yum install git python
sudo yum install python-pip
pip install boto3
aws configure
git clone https://github.com/aws-samples/amazon-guardduty-multiaccount-scripts.git
cd amazon-guardduty-multiaccount-scripts
sudo chmod +x disableguardduty.py enableguardduty.py
```

5. Crie um arquivo CSV que contenha uma lista de IDs e e-mails das contas-membro às quais você adicionou uma função na etapa 2. As contas devem aparecer uma por linha, e o ID da conta e o endereço de e-mail devem ser separados por vírgula, como no exemplo a seguir.

```
111122223333,guardduty-member@organization.com
```

> **Note**
>
> O arquivo CSV deve estar no mesmo local do script `enableguardduty.py`. É possível copiar um arquivo CSV existente do Amazon S3 no diretório atual com o método a seguir.
>
> ```
> aws s3 cp s3://my-bucket/my_key_name example.csv
> ```

6. Execute o script do Python. Certifique-se de fornecer o ID da conta do GuardDuty administrador, o nome da função criada nas primeiras etapas e o nome do seu arquivo CSV como argumentos.

```
python enableguardduty.py --master_account 444455556666 --assume_role
 roleName accountID.csv
```

Estimando GuardDuty o custo

Você pode usar o GuardDuty console ou as operações da API para estimar os custos médios diários de uso do GuardDuty. Durante o período de teste gratuito de 30 dias, a estimativa de custo projeta quais serão seus custos estimados após o período de teste. Se você estiver operando em um ambiente com várias contas, sua conta de GuardDuty administrador poderá monitorar as métricas de custo de todas as contas dos membros.

Você pode visualizar a estimativa de custo com base nas seguintes métricas:

- ID da conta — Lista o custo estimado para sua conta ou para suas contas de membros, se você estiver operando como uma conta de GuardDuty administrador.
- Fonte de dados — lista o custo estimado na fonte de dados especificada para os seguintes tipos de fonte de GuardDuty dados: registros de fluxo de VPC, registros de CloudTrail gerenciamento, eventos de CloudTrail dados ou registros de DNS.
- Recursos — Lista o custo estimado na fonte de dados especificada para os seguintes GuardDuty recursos: eventos de dados para S3, monitoramento do registro de auditoria do EKS, CloudTrail dados de volume do EBS, atividade de login do RDS, monitoramento do tempo de execução do EKS, monitoramento do tempo de execução do EKS, monitoramento do tempo de execução do Fargate, monitoramento do tempo de execução do EC2 ou monitoramento de atividades da rede Lambda.
- Buckets do S3: lista o custo estimado dos eventos de dados do S3 em um bucket especificado ou os buckets mais caros para contas em seu ambiente.

> **Note**
>
> As estatísticas de buckets do S3 só estão disponíveis se a Proteção do S3 estiver habilitada para a conta. Para ter mais informações, consulte Proteção do Amazon S3 na Amazon GuardDuty.

Entendendo como GuardDuty calcula os custos de uso

As estimativas exibidas no GuardDuty console podem ser um pouco diferentes das do seu AWS Billing and Cost Management console. A lista a seguir explica como GuardDuty estimar os custos de uso:

- A estimativa GuardDuty de uso é somente para a região atual.
- Durante o teste gratuito de 30 dias, a estimativa de GuardDuty uso é baseada nos últimos 7 a 30 dias de uso.

> **Note**
>
> Se a duração do uso GuardDuty ou de um recurso dentro dele GuardDuty for inferior a 7 dias, o valor do uso será mostrado como ***Moeda*** 0,00.

- A estimativa de custo de uso do teste inclui a estimativa de recursos e fontes de dados fundamentais que estão atualmente no período de teste. Cada recurso e fonte de dados dentro deles GuardDuty tem seu próprio período de teste, mas ele pode se sobrepor ao período de teste do GuardDuty ou a outro recurso que foi ativado ao mesmo tempo.
- A estimativa de GuardDuty uso inclui descontos nos preços por GuardDuty volume por região, conforme detalhado na página de GuardDuty preços da Amazon, mas somente para contas individuais que atendam aos níveis de preços por volume. Os descontos nos preços por volume não estão incluídos nas estimativas de uso total combinado entre contas dentro de uma organização. Para obter informações sobre preços de desconto por volume de uso combinado, consulte Faturamento da AWS : descontos por volume.

Monitoramento do tempo de execução — Como os registros de fluxo de VPC das instâncias do EC2 afetam o custo de uso

Quando você gerencia o agente de segurança (manualmente ou por meio de GuardDuty) no EKS Runtime Monitoring ou Runtime Monitoring para instâncias EC2, e atualmente GuardDuty está implantado em uma instância Tipos de eventos de runtime coletados do Amazon EC2 e os recebe dessa instância, não GuardDuty cobrará pela análise dos registros de fluxo Conta da AWS de VPC dessa instância do Amazon EC2. Isso ajuda a GuardDuty evitar o dobro do custo de uso na conta.

Como GuardDuty estima o custo de uso para CloudTrail eventos

Quando você ativa GuardDuty, ele começa automaticamente a consumir registros de AWS CloudTrail eventos registrados para sua conta no selecionado Região da AWS. GuardDuty replica os registros de eventos do serviço global e, em seguida, processa esses eventos de forma independente em cada região em que você GuardDuty ativou. Isso ajuda a GuardDuty manter perfis de usuário e função em cada região para identificar anomalias.

Sua CloudTrail configuração não afeta o custo GuardDuty de uso ou a forma como GuardDuty processa seus registros de eventos. Seu custo GuardDuty de uso é afetado pelo uso de AWS APIs que fazem login em CloudTrail. Para ter mais informações, consulte AWS CloudTrail registros de eventos.

Revisando estatísticas GuardDuty de uso

Escolha seu método de acesso preferido para revisar as estatísticas de uso GuardDuty da sua conta. Se você for uma conta de GuardDuty administrador, os métodos a seguir ajudarão você a analisar as estatísticas de uso de todos os membros.

Console

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.

   Certifique-se de usar a conta de GuardDuty administrador.
2. No painel de navegação, selecione Uso.
3. Na página Uso, uma conta de GuardDuty administrador com contas de membros pode ver o custo estimado da organização nos últimos 30 dias. Esse é um custo total de uso estimado para sua organização.
4. GuardDuty contas de administrador com membros podem visualizar o detalhamento do custo de uso por fonte de dados ou por contas. Contas individuais ou autônomas podem visualizar o detalhamento por fonte de dados.

   Se você tiver contas de membros, poderá visualizar as estatísticas de uma conta individual selecionando essa conta na tabela Contas.

API/CLI

Execute a operação GetUsageStatisticsda API usando as credenciais da conta do GuardDuty administrador. Forneça as seguintes informações para executar o comando:

- (Obrigatório) forneça o ID do GuardDuty detector regional da conta para a qual você deseja recuperar as estatísticas.
- (Obrigatório) Forneça um dos tipos de estatísticas para recuperar: `SUM_BY_ACCOUNT | SUM_BY_DATA_SOURCE | SUM_BY_RESOURCE | SUM_BY_FEATURE | TOP_ACCOUNTS_BY_FEATURE`.

Atualmente, `TOP_ACCOUNTS_BY_FEATURE` não oferece suporte à recuperação de estatísticas de uso do. `RDS_LOGIN_EVENTS`

- (Obrigatório) forneça uma ou mais fontes de dados ou recursos para consultar suas estatísticas de uso.
- (Opcional) Forneça uma lista de IDs de conta para as quais você deseja recuperar estatísticas de uso.

Você também pode usar o AWS Command Line Interface O comando a seguir é um exemplo sobre como recuperar as estatísticas de uso de todas as fontes de dados e recursos, calculadas por contas. Certifique-se de substituir `detector-id` por seu próprio ID de detector válido. Para contas autônomas, esse comando retorna o custo de uso dos últimos 30 dias relacionado apenas à sua conta. Se você for uma conta de GuardDuty administrador com contas de membros, verá os custos listados por conta para todos os membros.

Para encontrar a opção `detectorId` para sua conta e região atual, consulte a página de configurações no console https://console.aws.amazon.com/guardduty/.

Substitua `SUM_BY_ACCOUNT` pelo tipo com o qual você deseja calcular as estatísticas de uso.

Para monitorar o custo somente das fontes de dados

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"DataSources":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_LOGS", "KUBERNETES_AUDIT_LOGS",
 "EC2_MALWARE_SCAN"]}'
```

Para monitorar o custo dos recursos

```
aws guardduty get-usage-statistics --detector-id 12abc34d567e8fa901bc2d34e56789f0
 --usage-statistic-type SUM_BY_ACCOUNT --usage-criteria '{"Features":
["FLOW_LOGS", "CLOUD_TRAIL", "DNS_LOGS", "S3_DATA_EVENTS", "EKS_AUDIT_LOGS",
 "EBS_MALWARE_PROTECTION", "RDS_LOGIN_EVENTS", "LAMBDA_NETWORK_LOGS",
 "EKS_RUNTIME_MONITORING", "FARGATE_RUNTIME_MONITORING", "EC2_RUNTIME_MONITORING"]}'
```

Segurança no Amazon GuardDuty

A segurança para com a nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se contará com um datacenter e uma arquitetura de rede criados para atender aos requisitos das organizações com as maiores exigências de segurança.

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

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores externos testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao GuardDuty, consulte Serviços da AWS no escopo por programa de conformidade.
- Segurança na nuvem: sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o GuardDuty. Ela mostra como configurar o GuardDuty para atender aos objetivos de segurança e conformidade. Saiba também como usar outros produtos da AWS que ajudam a monitorar e proteger os recursos do IAM.

Índice

Proteção de dados na Amazon GuardDuty

O modelo de responsabilidade AWS compartilhada de se aplica à proteção de dados na Amazon GuardDuty. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com GuardDuty ou Serviços da AWS usa o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se

você fornecer um URL para um servidor externo, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia em repouso

Todos os dados GuardDuty do cliente são criptografados em repouso usando soluções de AWS criptografia.

GuardDuty dados, como descobertas, são criptografados em repouso usando AWS Key Management Service (AWS KMS) usando chaves AWS próprias gerenciadas pelo cliente.

Criptografia em trânsito

GuardDuty analisa dados de log de outros serviços. O GuardDuty criptografa todos os dados em trânsito desses serviços com HTTPS e KMS. Depois de GuardDuty extrair as informações necessárias dos registros, elas são descartadas. Para obter mais informações sobre como GuardDuty usa as informações de outros serviços, consulte fontes GuardDuty de dados.

GuardDuty os dados são criptografados em trânsito entre os serviços.

Optar por não usar seus dados para melhorar o serviço

Você pode optar por não ter seus dados usados para desenvolver GuardDuty e melhorar outros serviços AWS de segurança usando a política de AWS Organizations exclusão. Você pode optar por não coletar nenhum desses dados, mesmo GuardDuty que atualmente não colete nenhum desses dados. Para obter mais informações sobre como optar por não participar, consulte as políticas de exclusão dos serviços de IA no Guia do usuário do AWS Organizations .

> **Note**
>
> Para que você possa usar a política de exclusão, suas AWS contas devem ser gerenciadas centralmente pelo. AWS Organizations Se você ainda não criou uma organização para suas AWS contas, consulte Criação e gerenciamento de uma organização no Guia do AWS Organizations usuário.

A exclusão tem os seguintes efeitos:

- GuardDuty excluirá os dados coletados e armazenados para fins de melhoria do serviço antes de sua exclusão (se houver).

- Depois de optar por não participar, não GuardDuty coletará nem armazenará mais esses dados para fins de melhoria do serviço.

Os tópicos a seguir explicam como cada recurso interno GuardDuty potencialmente manipula seus dados para melhorar o serviço.

Conteúdo

GuardDuty Monitoramento de execução

GuardDuty O Runtime Monitoring fornece detecção de ameaças em tempo de execução para clusters do Amazon Elastic Kubernetes Service (Amazon EKS) AWS Fargate (Fargate) , somente para o Amazon Elastic Container Service (Amazon ECS) e para instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em seu ambiente. AWS Depois de habilitar o Runtime Monitoring e implantar o agente de GuardDuty segurança para seu recurso, GuardDuty começa a monitorar e analisar os eventos de tempo de execução associados ao seu recurso. Esses tipos de eventos de tempo de execução incluem eventos de processo, eventos de contêiner, eventos de DNS e muito mais. Para ter mais informações, consulte Tipos de eventos de tempo de execução coletados que GuardDuty usam.

Embora GuardDuty agora colete argumentos de linha de comando que você pode direcionar para suas cargas de trabalho, atualmente ele não usa esses argumentos para fins de melhoria de serviços (talvez o faça no futuro). Começamos a coletar argumentos de linha de comando em antecipação às novas regras e descobertas de detecção de ameaças que serão lançadas em breve. Sua confiança, privacidade e segurança de seu conteúdo são nossa maior prioridade e garantem que nosso uso esteja em conformidade com nossos compromissos com você. Para obter mais informações, consulte Perguntas frequentes sobre a privacidade de dados.

GuardDuty Proteção contra malware

GuardDuty A Proteção contra Malware verifica e detecta malware contido em volumes do EBS anexados à sua instância do Amazon EC2 e cargas de trabalho de contêineres potencialmente comprometidas. Quando a Proteção contra GuardDuty Malware identifica um arquivo de volume do EBS como sendo malicioso ou prejudicial, a Proteção contra GuardDuty Malware coleta e armazena esse arquivo para desenvolver e melhorar suas detecções de malware e o serviço. GuardDuty Esse

arquivo também pode ser usado para desenvolver e melhorar outros serviços AWS de segurança. Sua confiança, privacidade e segurança de seu conteúdo são nossa maior prioridade e garantem que nosso uso esteja em conformidade com nossos compromissos com você. Para obter mais informações, consulte Perguntas frequentes sobre a privacidade de dados.

Registrando chamadas de GuardDuty API da Amazon com AWS CloudTrail

GuardDuty A Amazon está integrada comAWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço em GuardDuty. CloudTrail captura todas as chamadas de API para GuardDuty eventos As, incluindo chamadas do GuardDuty console e de chamadas de código para as GuardDuty APIs. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon Simple Storage Service (Amazon S3), incluindo eventos para. GuardDuty Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita GuardDuty, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para obter mais informações sobre CloudTrail, inclusive como configurá-lo e ativá-lo, consulte o Guia AWS CloudTrail do usuário.

GuardDuty informações em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando uma atividade de evento suportada ocorre em GuardDuty, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos para GuardDuty, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, ao criar uma trilha no console, a mesma é aplicada a todas as Regiões. A trilha registra logs de eventos de todas as Regiões na AWS divisória e entrega os arquivos do log para o bucket Amazon S3 especificado. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha

- Serviços e integrações compatíveis com o CloudTrail
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou de usuário do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado
- Se a solicitação foi feita por outro serviço da AWS

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

GuardDuty eventos do plano de controle em CloudTrail

Por padrão, CloudTrail registra todas as operações de GuardDuty API fornecidas na Amazon GuardDuty API Reference como eventos em CloudTrail arquivos.

GuardDuty eventos de dados em CloudTrail

GuardDuty Monitoramento de execuçãousa um agente de GuardDuty segurança implantado em seus clusters do Amazon Elastic Kubernetes Service (Amazon EKS), instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e `aws-guardduty-agent` tarefas (somente Amazon AWS Fargate Elastic Container Service (Amazon ECS)) para coletar Tipos de eventos de runtime coletados complementos () que coletam para suas cargas de trabalho e, em seguida, enviá-las para detecção de ameaças e análise. AWS GuardDuty

Registro e monitoramento de eventos de dados

Opcionalmente, você pode configurar os AWS CloudTrail registros para visualizar os eventos de dados do seu agente GuardDuty de segurança.

Para criar e configurar CloudTrail, consulte Eventos de dados no Guia do AWS CloudTrail usuário e siga as instruções para registrar eventos de dados com seletores de eventos avançados no AWS Management Console. Ao registrar a trilha em log, faça as seguintes alterações:

- Para o tipo de evento de dados, escolha GuardDuty detector.
- Para o Modelo do seletor de logs, escolha Registrar todos os eventos em log.
- Expanda a Visualização JSON da configuração. Ela deve ser semelhante à indicada a seguir.

```
[
  {
    "name": "",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
          "AWS::GuardDuty::Detector"
        ]
      }
    ]
  }
]
```

Depois de habilitar o seletor para a trilha, navegue até o console do Amazon S3 em https://console.aws.amazon.com/s3/. Você pode baixar os eventos de dados do bucket do S3 escolhido no momento da configuração dos CloudTrail registros.

Exemplo: entradas do arquivo de GuardDuty log

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra o evento do plano de dados.

```
{
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "111122223333:aws:ec2-instance:i-123412341234example",
            "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-
instance/i-123412341234example",
            "accountId": "111122223333",
            "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "111122223333:aws:ec2-instance",
                    "arn": "arn:aws:iam::111122223333:role/aws:ec2-instance",
                    "accountId": "111122223333",
                    "userName": "aws:ec2-instance"
                },
                "attributes": {
                    "creationDate": "2023-03-05T04:00:21Z",
                    "mfaAuthenticated": "false"
                },
                "ec2RoleDelivery": "2.0"
            }
        },
        "eventTime": "2023-03-05T06:03:49Z",
        "eventSource": "guardduty.amazonaws.com",
        "eventName": "SendSecurityTelemetry",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "54.240.230.177",
        "userAgent": "aws-sdk-rust/0.54.1 os/linux lang/rust/1.66.0",
        "requestParameters": null,
        "responseElements": null,
        "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
        "readOnly": false,
        "resources": [{
            "accountId": "111122223333",
            "type": "AWS::GuardDuty::Detector",
            "ARN": "arn:aws:guardduty:us-
west-2:111122223333:detector/12abc34d567e8fa901bc2d34e56789f0"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
```

```
        "recipientAccountId": "111122223333",
        "eventCategory": "Data",
        "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "guardduty-data.us-east-1.amazonaws.com"
        }
    }
```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `CreateIPThreatIntelSet` ação (evento do plano de controle).

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-06-14T22:54:20Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2018-06-14T22:57:56Z",
    "eventSource": "guardduty.amazonaws.com",
    "eventName": "CreateThreatIntelSet",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.240.230.177",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "detectorId": "12abc34d567e8fa901bc2d34e56789f0",
        "name": "Example",
```

```
        "format": "TXT",
        "activate": false,
        "location": "https://s3.amazonaws.com/bucket.name/file.txt"
    },
    "responseElements": {
        "threatIntelSetId": "1ab200428351c99d859bf61992460d24"
    },
    "requestID": "5f6bf981-7026-11e8-a9fc-5b37d2684c5c",
    "eventID": "81337b11-e5c8-4f91-b141-deb405625bc9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "444455556666"
}
```

A partir das informações desse evento, você pode determinar que a solicitação foi feita para criar uma lista de ameaças `Example` no GuardDuty. Você também pode ver que a solicitação foi feita por uma usuária chamada Alice em 14 de junho de 2018.

Identity and Access Management para Amazon GuardDuty

AWS Identity and Access Management (IAM) é um serviço da AWS service (Serviço da AWS) que ajuda o administrador no controle de segurança de acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar GuardDuty os recursos. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

Tópicos

Público

O uso do AWS Identity and Access Management (IAM) varia dependendo do trabalho que for realizado no GuardDuty.

Usuário do serviço — Se você usar o GuardDuty serviço para realizar seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais GuardDuty recursos para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um recurso no GuardDuty, consulte Solução de problemas de GuardDuty identidade e acesso da Amazon.

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

Administrador do IAM – Se você for um administrador do IAM, talvez queira saber detalhes sobre como pode gravar políticas para gerenciar acesso ao GuardDuty. Para ver exemplos de políticas GuardDuty baseadas em identidade que você pode usar no IAM, consulte. Exemplos de políticas baseadas em identidade para a Amazon GuardDuty

Como autenticar com identidades

A autenticação é a forma como você faz login na AWS usando suas credenciais de identidade. Você deve ser autenticado (ter feito login em AWS) como o usuário raiz da Usuário raiz da conta da AWS, como usuário do IAM ou assumindo um perfil do IAM.

Você pode ter feito login em AWS como uma identidade federada usando credenciais fornecidas por meio de origem de identidade. AWS IAM Identity Center Os usuários do IAM Identity Center [Centro de Identidade], a autenticação única da empresa e as suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Quando você acessa a AWS usando a federação, está indiretamente assumindo um perfil.

A depender do tipo de usuário que você seja, você pode fazer login no AWS Management Console ou no portal de acesso da AWS. Para obter mais informações sobre como fazer login em AWS, consulte Como Fazer Login na sua Conta da AWS no Início de Sessão da AWS Manual do usuário.

Se você acessar AWS programaticamente, a AWS fornecerá um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando as suas credenciais. Se você não utilizar as ferramentas da AWS, deverá assinar as solicitações por conta própria. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinando Solicitações de API AWS noGuia do Usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte Autenticação Multifator no AWS IAM Identity CenterGuia do Usuário. Usar a autenticação multifator (MFA) na AWS no Guia do Usuário do IAM.

Usuário raiz da Conta da AWS

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos os recursos e Serviços da AWS na conta. Essa identidade, denominada usuário raiz da Conta da AWS, e é acessada por login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários - inclusive os que precisem de acesso administrativo - usem a federação com um provedor de identidades para acessar Serviços da AWS usando credenciais temporárias.

Identidade federada é um usuário de seu diretório de usuários corporativos, um provedor de identidades web, o AWS Directory Service, o Diretório do Identity Center ou qualquer usuário que acesse os Serviços da AWS usando credenciais fornecidas por meio de uma origem de identidade. Quando as identidades federadas acessam Contas da AWS, elas assumem perfis que fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no Centro de Identidade do IAM ou se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todas as suas Contas da AWS e aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no AWS IAM Identity CenterManual do Usuário do.

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos depender de credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne 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 nome de grupo 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 um aplicativo, mas uma função pode ser assumida por qualquer pessoa que precisar dela. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando Criar um Usuário do IAM (Ao Invés de uma Função) no Guia do Usuário do IAM.

Perfis do IAM

Um perfil do IAM é uma identidade dentro da Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. É possível assumir temporariamente um perfil do IAM em AWS Management Console alternando perfis. É possível assumir um perfil chamando uma operação de API da AWS CLI ou da AWS, ou mesmo usando URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte Usando Funções do IAM no Guia do Usuário do IAM.

Funções 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 Criando um Perfil para um Provedor de Identidades Terceirizado no Guia do Usuário do IAM. Se você usa 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 CenterManual do Usuário.
- Permissões de usuários temporárias do IAM –- um usuário ou perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas –- você pode usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) acesse recursos na sua conta de uma conta diferente. As funções são a forma primária 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 aprender 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 aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões de chamada da entidade principal, uma função de serviço ou uma função vinculada ao serviço.
  - Encaminhamento de sessões de acesso (FAS): qualquer pessoa que utilizar uma função ou usuário do IAM para realizar ações na AWS é considerada uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você deve ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhamento de sessões de acesso.
  - Função de Serviço –- uma função de serviço é uma função 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 Criando um Perfil para Delegar Permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

- Função vinculada a serviço –- uma função vinculada a serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode assumir o perfil de executar uma ação em seu nome. Funções vinculadas ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas a serviço.

- Aplicações em execução no Amazon EC2: é possível usar uma função do IAM para gerenciar credenciais temporárias para aplicativos em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma função da AWS a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, crie um perfil de instância que esteja anexado a ela. 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 aplicativos em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para aprender se deseja usar perfis do IAM, consulte Quando Criar uma Função do IAM (em Vez de um Usuário) no Guia do Usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as a identidades ou recursos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou recurso, define suas permissões. A AWS avalia essas políticas quando uma entidade 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 são armazenadas na 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 as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e sob quais condições.

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

As políticas do IAM definem permissões para uma ação, independente 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 perfis do AWS Management Console, da AWS CLI ou da API da AWS.

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 quais 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 também podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são incorporadas diretamente a um único usuário, grupo ou função. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e perfis na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS e políticas gerenciadas pelo cliente. Para saber como selecionar entre uma política gerenciada ou uma política em linha, consulte Selecionar 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 função do IAM e as políticas do bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

Políticas baseadas em recursos são políticas em linha que estão localizadas nesse serviço. Não é possível usar as políticas gerenciadas da AWS 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 permissão para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

Amazon S3, AWS WAF e Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. Saiba mais sobre ACLs em Configurações da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

A AWS oferece suporte a tipos de política 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 perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de Permissões para Entidades 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 (UO) no AWS Organizations. O AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS pertencentes à sua empresa. 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 em contas-membro, inclusive cada Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte Como os SCPs Funcionam no AWS OrganizationsManual 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. Saiba como a AWS determina se deve permitir uma solicitação quando há vários tipos de política envolvidos consultando Lógica da Avaliação de Políticas no Guia do Usuário do IAM.

Como a Amazon GuardDuty trabalha com o IAM

Antes de usar o IAM para gerenciar o acesso GuardDuty, saiba com quais recursos do IAM estão disponíveis para uso GuardDuty.

Recursos do IAM que você pode usar com a Amazon GuardDuty

Atributos do IAM	GuardDuty apoio
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC (etiquetas em políticas)	Parcial
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Sim
Funções vinculadas a serviço	Sim

Para ter uma visão de alto nível de como GuardDuty e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWSos serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para GuardDuty

Suporta com políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário IAM, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em quais condições. Saiba como criar uma política baseada em identidade consultando Criando Políticas do IAM no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou função à qual ela está anexada. Saiba mais sobre todos os elementos que podem ser usados em uma política JSON consultando Referência de Elementos de Política JSON do IAM no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade para GuardDuty

Para ver exemplos de políticas GuardDuty baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para a Amazon GuardDuty

Políticas baseadas em recursos dentro GuardDuty

Oferece suporte a políticas baseadas em recursos	Não

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 função do IAM e as políticas do bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para

o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. As entidades principais podem incluir contas, usuários, funções, usuários federados ou Serviços da AWS.

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recurso. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando a entidade principal e o recurso estão em diferentes Contas da AWS, um administrador do IAM da conta confiável também deve conceder à entidade principal (usuário ou perfil) permissão para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Ações políticas para GuardDuty

Oferece suporte a ações de políticas	Sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a 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 políticas geralmente têm o mesmo nome que a operação de API da AWS associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de GuardDuty ações, consulte Ações definidas pela Amazon GuardDuty na Referência de autorização de serviço.

As ações de política GuardDuty usam o seguinte prefixo antes da ação:

```
guardduty
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
      "guardduty:action1",
      "guardduty:action2"
         ]
```

Para ver exemplos de políticas GuardDuty baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para a Amazon GuardDuty

Recursos políticos para GuardDuty

Oferece suporte a recursos de políticas	Sim

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a 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 de 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 curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para ver uma lista dos tipos de GuardDuty recursos e seus ARNs, consulte Recursos definidos pela Amazon GuardDuty na Referência de autorização de serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pela Amazon. GuardDuty

Para ver exemplos de políticas GuardDuty baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para a Amazon GuardDuty

Chaves de condição de política para GuardDuty

Suporta chaves de condição de política específicas de serviço	Sim

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

O elemento `Condition` (ou bloco `Condition`) permite especificar condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. Você pode criar expressões condicionais que usem operadores de condição, como “igual a” ou “menor que”, para corresponder a condição da política aos valores na solicitação.

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

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, 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.

A AWS oferece suporte a chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição globais da AWS, consulte AWSChaves de Contexto de Condição Globais da no Guia do Usuário do IAM.

Para ver uma lista de chaves de GuardDuty condição, consulte Chaves de condição da Amazon GuardDuty na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pela Amazon GuardDuty.

Para ver exemplos de políticas GuardDuty baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para a Amazon GuardDuty

Listas de controle de acesso (ACLs) em GuardDuty

Oferece suporte a ACLs	Não

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

Controle de acesso baseado em atributos (ABAC) com GuardDuty

Oferece suporte a ABAC (tags em políticas)	Parcial

O controle de acesso baseado em atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Na AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a muitos recursos da AWS. A marcação de entidades e recursos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre a tag no elemento de condição de uma política usando as chaves de condição `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial.

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com GuardDuty

Oferece suporte a credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para informações adicionais, inclusive quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS que Funcionam com o IAM no Guia do Usuário do IAM.

Você estará usando credenciais temporárias se fizer login no AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa a AWS usando o link de autenticação única (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para uma Função (Console) no Guia do Usuário do IAM.

Você pode criar credenciais temporárias de forma manual usando a AWS CLI ou a API da AWS. Em seguida, você pode usar essas credenciais temporárias para acessar a AWS. A AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Permissões principais entre serviços para GuardDuty

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou perfil do IAM para executar ações na AWS, você é considerado uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. Nesse caso, você deve ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhamento de sessões de acesso.

Funções de serviço para GuardDuty

Suporta perfis de serviço	Sim

A função de serviço é uma função do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criando um Perfil para Delegar Permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper GuardDuty a funcionalidade. Edite as funções de serviço somente quando GuardDuty fornecer orientação para fazer isso.

Funções vinculadas a serviços para GuardDuty

Oferece suporte a perfis vinculados ao serviço	Sim

Uma função vinculada ao serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode assumir a função de executar uma ação em seu nome. Funções vinculadas ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas a serviço.

Para obter detalhes sobre como criar ou gerenciar funções GuardDuty vinculadas a serviços, consulte. Usando funções vinculadas a serviços para a Amazon GuardDuty

Para obter detalhes sobre como criar ou gerenciar funções vinculadas a serviços, consulte AWSServiços que Funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Função Vinculada ao Serviço.. Selecione o link Sim para visualizar a documentação da função vinculada a serviço desse serviço.

Exemplos de políticas baseadas em identidade para a Amazon GuardDuty

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do GuardDuty. Eles também não podem executar tarefas usando o AWS Management Console, a AWS Command Line Interface (AWS CLI) ou a AWS API. Para conceder permissões de usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a funções, e os usuários podem assumir as funções.

Saiba como criar uma política baseada em identidade do IAM usando esses exemplos de documento da política JSON consultando Criando Políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos por GuardDuty, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para a Amazon GuardDuty na Referência de Autorização de Serviço.

Tópicos

Melhores práticas de políticas

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

- Comece a usar as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo –- para começar a conceder permissões a seus usuários e workloads, use as políticas gerenciadas pela AWS que concedem permissões para muitos casos de uso comuns. Elas estão disponíveis em seus Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente específicas para seus casos de uso. Para obter mais informações, consulte Políticas Gerenciadas pela AWS ou AWS Políticas Gerenciadas 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.
- Utilize 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 gravar uma condição de política para especificar que todas as solicitações devem ser enviadas

usando SSL. Você também pode usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um AWS service (Serviço da AWS) específico, como o AWS CloudFormation. Para obter mais informações, consulte Condição de Elementos de Política JSON do IAM no Guia do Usuário do IAM.

- Use o IAM Access Analyzer para validar suas políticas do IAM para garantir permissões seguras e funcionais –- o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam o idioma de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e ações recomendadas para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de Política do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA): se houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configurando Acesso à API Protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas Recomendadas de Segurança no IAM no Guia do Usuário do IAM.

Utilizando o console do GuardDuty

Para acessar o GuardDuty console da Amazon, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os GuardDuty recursos em seuConta da AWS. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou funções) com essa política.

Não é necessário conceder permissões mínimas do console para usuários fazendo chamadas somente para AWS CLI ou para a API do AWS. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o GuardDuty console, anexe também a política GuardDuty `ConsoleAccess` ou a política `ReadOnly` AWS gerenciada às entidades. Para obter mais informações, consulte Adicionando Permissões a um Usuário no Guia do Usuário do IAM.

Permissões necessárias para habilitar o GuardDuty

Para conceder permissões que várias identidades do IAM (usuários, grupos e funções) devem ter, anexe a AWS política gerenciada: AmazonGuardDutyFullAccess política necessária para GuardDuty habilitar.

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou de forma programática usando a AWS CLI ou a API da AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

Política personalizada do IAM para conceder acesso somente de leitura ao GuardDuty

Para conceder acesso somente de leitura, GuardDuty você pode usar a política `AmazonGuardDutyReadOnlyAccess` gerenciada.

Para criar uma política personalizada que conceda acesso somente para leitura a uma função, usuário ou grupo do IAM GuardDuty, você pode usar a seguinte declaração:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ListMembers",
                "guardduty:GetMembers",
                "guardduty:ListInvitations",
                "guardduty:ListDetectors",
                "guardduty:GetDetector",
                "guardduty:ListFindings",
                "guardduty:GetFindings",
                "guardduty:ListIPSets",
                "guardduty:GetIPSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:GetThreatIntelSet",
                "guardduty:GetMasterAccount",
                "guardduty:GetInvitationsCount",
                "guardduty:GetFindingsStatistics",
                "guardduty:DescribeMalwareScans",
                "guardduty:UpdateMalwareScanSettings",
                "guardduty:GetMalwareScanSettings"
            ],
            "Resource": "*"
        }
    ]
}
```

Negar acesso às GuardDuty descobertas

Você pode usar a política a seguir para negar acesso às GuardDuty descobertas de uma função, usuário ou grupo do IAM. Os usuários não podem ver as descobertas ou os detalhes sobre as descobertas, mas podem acessar todas as outras GuardDuty operações:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:CreateDetector",
                "guardduty:DeleteDetector",
                "guardduty:UpdateDetector",
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "guardduty:CreateIPSet",
                "guardduty:DeleteIPSet",
                "guardduty:UpdateIPSet",
                "guardduty:GetIPSet",
                "guardduty:ListIPSets",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:UpdateThreatIntelSet",
                "guardduty:GetThreatIntelSet",
                "guardduty:ListThreatIntelSets",
                "guardduty:ArchiveFindings",
                "guardduty:UnarchiveFindings",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateMembers",
                "guardduty:InviteMembers",
                "guardduty:GetMembers",
                "guardduty:DeleteMembers",
                "guardduty:DisassociateMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:ListMembers",
                "guardduty:GetMasterAccount",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:AcceptAdministratorInvitation",
                "guardduty:ListInvitations",
                "guardduty:GetInvitationsCount",
```

```
                "guardduty:DeclineInvitations",
                "guardduty:DeleteInvitations"
            ],
            "Resource": "*"
        },
         {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
        }
    ]
}
```

Usando uma política personalizada do IAM para limitar o acesso aos GuardDuty recursos

Para definir o acesso de um usuário GuardDuty com base no ID do detector, você pode usar todas as ações de GuardDuty API em suas políticas personalizadas do IAM, exceto as seguintes operações:

- `guardduty:CreateDetector`
- `guardduty:DeclineInvitations`
- `guardduty:DeleteInvitations`
- `guardduty:GetInvitationsCount`

- `guardduty:ListDetectors`
- `guardduty:ListInvitations`

Use as seguintes operações em uma política do IAM para definir o acesso de um usuário GuardDuty com base no ID e no ID do IPset ThreatIntelSet :

- `guardduty:DeleteIPSet`
- `guardduty:DeleteThreatIntelSet`
- `guardduty:GetIPSet`
- `guardduty:GetThreatIntelSet`
- `guardduty:UpdateIPSet`
- `guardduty:UpdateThreatIntelSet`

Os exemplos a seguir mostram como criar políticas usando algumas das operações anteriores:

- Esta política permite que um usuário execute a operação `guardduty:UpdateDetector` usando o ID do detector de 1234567 na região us-east-1:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateDetector",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567"
        }
    ]
}
```

- Esta política permite que um usuário execute a operação `guardduty:UpdateIPSet` usando o ID do detector de 1234567 e o ID de IPSet de 000000 na região us-east-1:

> **Note**
>
> Certifique-se de que o usuário tenha as permissões necessárias para acessar listas de IP confiáveis e listas de ameaças em GuardDuty. Para obter mais informações, consulte Permissões necessárias para fazer upload das listas de IP confiáveis e listas de ameaças.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
             ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/000000"
        }
    ]
}
```

- Esta política permite que um usuário execute a operação `guardduty:UpdateIPSet` usando qualquer ID de detector e o ID de IPSet de 000000 na região us-east-1:

> **Note**
>
> Certifique-se de que o usuário tenha as permissões necessárias para acessar listas de IP confiáveis e listas de ameaças em GuardDuty. Para obter mais informações, consulte Permissões necessárias para fazer upload das listas de IP confiáveis e listas de ameaças.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                 "guardduty:UpdateIPSet",
```

```
            ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/*/
ipset/000000"
        }
    ]
}
```

- Esta política permite que um usuário execute a operação `guardduty:UpdateIPSet` usando o ID de detector e qualquer ID de IPSet na região us-east-1:

> **Note**
>
> Certifique-se de que o usuário tenha as permissões necessárias para acessar listas de IP confiáveis e listas de ameaças em GuardDuty. Para obter mais informações, consulte Permissões necessárias para fazer upload das listas de IP confiáveis e listas de ameaças.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:UpdateIPSet",
            ],
            "Resource": "arn:aws:guardduty:us-east-1:123456789012:detector/1234567/
ipset/*"
        }
    ]
}
```

Usando funções vinculadas a serviços para a Amazon GuardDuty

A Amazon GuardDuty usa AWS Identity and Access Management funções vinculadas a serviços (IAM). Uma função vinculada ao serviço (SLR) é um tipo exclusivo de função do IAM vinculada diretamente a. GuardDuty As funções vinculadas ao serviço são predefinidas GuardDuty e incluem todas as permissões GuardDuty necessárias para chamar outros AWS serviços em seu nome.

Com a função vinculada ao serviço, você pode configurar GuardDuty sem adicionar manualmente as permissões necessárias. GuardDuty define as permissões de sua função vinculada ao serviço e,

a menos que as permissões sejam definidas de outra forma, somente GuardDuty pode assumir a função. As permissões definidas incluem a política de confiança e a política de permissões, e essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

GuardDuty suporta o uso de funções vinculadas a serviços em todas as regiões em que GuardDuty está disponível. Para ter mais informações, consulte Regiões e endpoints.

Você pode excluir a função GuardDuty vinculada ao serviço somente após a primeira desativação GuardDuty em todas as regiões em que ela está ativada. Isso protege seus GuardDuty recursos porque você não pode remover inadvertidamente a permissão para acessá-los.

Para obter informações sobre outros serviços que oferecem suporte a funções vinculadas a serviços, consulte AWS serviços que funcionam com o IAM no Guia do usuário do IAM e procure os serviços que têm Sim na coluna Função vinculada ao serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões de função vinculadas ao serviço para GuardDuty

GuardDuty usa a função vinculada ao serviço (SLR) chamada. `AWSServiceRoleForAmazonGuardDuty` A SLR permite GuardDuty realizar as seguintes tarefas. Também permite incluir GuardDuty os metadados recuperados pertencentes à instância do EC2 nas descobertas que GuardDuty podem gerar sobre a ameaça potencial. A função vinculada ao serviço `AWSServiceRoleForAmazonGuardDuty` confia no serviço `guardduty.amazonaws.com` para presumir a função.

As políticas de permissão ajudam a GuardDuty realizar as seguintes tarefas:

- Use as ações do Amazon EC2 para gerenciar e recuperar informações sobre suas instâncias, imagens e componentes de rede do EC2, como VPCs, sub-redes, gateways de trânsito e grupos de segurança.
- Use AWS Systems Manager ações para gerenciar associações de SSM em instâncias do Amazon EC2 ao GuardDuty ativar o Runtime Monitoring com um agente automatizado para o Amazon EC2. Quando a configuração GuardDuty automatizada do agente está desativada, GuardDuty considera somente as instâncias do EC2 que têm uma tag de inclusão (`GuardDutyManaged:true`).
- Use AWS Organizations ações para descrever contas associadas e ID da organização.
- Use as ações do Amazon S3 para recuperar informações sobre buckets e objetos do S3.
- Use AWS Lambda ações para recuperar informações sobre suas funções e tags do Lambda.

- Use as ações do Amazon EKS para gerenciar e recuperar informações sobre os clusters do EKS e gerenciar os complementos do Amazon EKS nos clusters do EKS. As ações do EKS também recuperam as informações sobre as tags associadas a. GuardDuty
- Use o IAM para criar o Permissões de função vinculada ao serviço para Proteção contra malware após a habilitação da Proteção contra malware.
- Use as ações do Amazon ECS para gerenciar e recuperar informações sobre os clusters do Amazon ECS e gerenciar a configuração da conta do Amazon ECS com. `guarddutyActivate` As ações relacionadas ao Amazon ECS também recuperam as informações sobre as tags associadas a. GuardDuty

A função é configurada com a seguinte política gerenciada da AWS, denominada `AmazonGuardDutyServiceRolePolicy`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GuardDutyGetDescribeListPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeTransitGatewayAttachments",
                "organizations:ListAccounts",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetEncryptionConfiguration",
                "s3:GetBucketTagging",
                "s3:GetAccountPublicAccessBlock",
                "s3:ListAllMyBuckets",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "lambda:GetFunctionConfiguration",
                "lambda:ListTags",
                "eks:ListClusters",
```

```
                "eks:DescribeCluster",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeSecurityGroups",
                "ecs:ListClusters",
                "ecs:DescribeClusters"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GuardDutyCreateSLRPolicy",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateVpcEndpointPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                },
                "StringLike": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.*.guardduty-data",
                        "com.amazonaws.*.guardduty-data-fips"
                    ]
                }
            }
        },
        {
            "Sid": "GuardDutyModifyDeleteVpcEndpointPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpoint",
                "ec2:DeleteVpcEndpoints"
            ],
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
```

```
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "GuardDutyCreateModifyVpcEndpointNetworkPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVpcEndpoint",
                "ec2:ModifyVpcEndpoint"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:vpc/*",
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:subnet/*"
            ]
        },
        {
             "Sid": "GuardDutyCreateTagsDuringVpcEndpointCreationPolicy",
             "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:vpc-endpoint/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateVpcEndpoint"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutySecurityGroupManagementPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
```

```
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyManaged": false
                }
            }
        },
        {
            "Sid": "GuardDutyCreateSecurityGroupPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/GuardDutyManaged": "*"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateSecurityGroupForVpcPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:vpc/*"
        },
        {
            "Sid": "GuardDutyCreateTagsDuringSecurityGroupCreationPolicy",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSecurityGroup"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyCreateEksAddonPolicy",
            "Effect": "Allow",
            "Action": "eks:CreateAddon",
            "Resource": "arn:aws:eks:*:*:cluster/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
```

```
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyEksAddonManagementPolicy",
            "Effect": "Allow",
            "Action": [
                "eks:DeleteAddon",
                "eks:UpdateAddon",
                "eks:DescribeAddon"
            ],
            "Resource": "arn:aws:eks:*:*:addon/*/aws-guardduty-agent/*"
        },
        {
            "Sid": "GuardDutyEksClusterTagResourcePolicy",
            "Effect": "Allow",
            "Action": "eks:TagResource",
            "Resource": "arn:aws:eks:*:*:cluster/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyManaged"
                }
            }
        },
        {
            "Sid": "GuardDutyEcsPutAccountSettingsDefaultPolicy",
            "Effect": "Allow",
            "Action": "ecs:PutAccountSettingDefault",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecs:account-setting": [
                        "guardDutyActivate"
                    ]
                 }
            }
        },
        {
            "Sid": "SsmCreateDescribeUpdateDeleteStartAssociationPermission",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeAssociation",
                "ssm:DeleteAssociation",
```

```
                "ssm:UpdateAssociation",
                "ssm:CreateAssociation",
                "ssm:StartAssociationsOnce"
            ],
            "Resource": "arn:aws:ssm:*:*:association/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/GuardDutyManaged": "true"
                }
            }
        },
        {
            "Sid": "SsmAddTagsToResourcePermission",
            "Effect": "Allow",
            "Action": [
                "ssm:AddTagsToResource"
            ],
            "Resource": "arn:aws:ssm:*:*:association/*",
            "Condition":{
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyManaged"
                    ]
                },
                "StringEquals": {
                    "aws:ResourceTag/GuardDutyManaged": "true"
                }
            }
        },
        {
            "Sid": "SsmCreateUpdateAssociationInstanceDocumentPermission",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateAssociation",
                "ssm:UpdateAssociation"
            ],
            "Resource": "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
        },
        {
            "Sid": "SsmSendCommandPermission",
            "Effect": "Allow",
            "Action": "ssm:SendCommand",
            "Resource": [
```

```
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ssm:*:*:document/AmazonGuardDuty-
ConfigureRuntimeMonitoringSsmPlugin"
            ]
        },
        {
            "Sid": "SsmGetCommandStatus",
            "Effect": "Allow",
            "Action": "ssm:GetCommandInvocation",
            "Resource": "*"
        }
    ]
}
```

Veja a seguir a política de confiança anexada à função vinculada a serviço `AWSServiceRoleForAmazonGuardDuty`:

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

Criação de uma função vinculada ao serviço para GuardDuty

A função `AWSServiceRoleForAmazonGuardDuty` vinculada ao serviço é criada automaticamente quando você a ativa GuardDuty pela primeira vez ou ativa GuardDuty em uma região compatível onde você não a tinha habilitada anteriormente. Você também pode criar a função vinculada ao serviço manualmente usando o console do IAM AWS CLI, o ou a API do IAM.

> **Important**
>
> A função vinculada ao serviço criada para a conta de administrador GuardDuty delegado não se aplica às contas dos membros. GuardDuty

É necessário configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para que a função `AWSServiceRoleForAmazonGuardDuty` vinculada ao serviço seja criada com sucesso, o principal do IAM GuardDuty com o qual você usa deve ter as permissões necessárias. Para conceder as permissões necessárias, anexe a seguinte política ao usuário, grupo ou função do :

> **Note**
>
> Substitua o exemplo de *`ID da conta`* no exemplo a seguir pelo seu ID de AWS conta real.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "guardduty.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty"
```

```
        }
    ]
}
```

Para mais informações sobre a criação da função manualmente, consulte Criar uma função vinculada ao serviço no Guia do usuário do IAM.

Editando uma função vinculada ao serviço para GuardDuty

GuardDuty não permite que você edite a função `AWSServiceRoleForAmazonGuardDuty` vinculada ao serviço. Depois que você criar um perfil vinculado ao serviço, não poderá alterar o nome do perfil, pois várias entidades podem fazer referência ao perfil. No entanto, você poderá 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.

Excluindo uma função vinculada ao serviço para GuardDuty

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 terá uma entidade não utilizada que não seja monitorada ativamente ou mantida.

> **Important**
>
> Se você habilitou a Proteção contra malware, a exclusão `AWSServiceRoleForAmazonGuardDuty` não é excluída `AWSServiceRoleForAmazonGuardDutyMalwareProtection` automaticamente. Se você deseja excluir `AWSServiceRoleForAmazonGuardDutyMalwareProtection`, consulte Excluir uma função vinculada ao serviço para a Proteção contra malware.

Você deve primeiro desabilitar GuardDuty em todas as regiões em que está habilitado para excluir `AWSServiceRoleForAmazonGuardDuty` o. Se o GuardDuty serviço não for desativado quando você tentar excluir a função vinculada ao serviço, a exclusão falhará. Para ter mais informações, consulte Suspendendo ou desativando GuardDuty.

Quando você desativa GuardDuty, o `AWSServiceRoleForAmazonGuardDuty` não é excluído automaticamente. Se você ativar GuardDuty novamente, ele começará a usar o existente`AWSServiceRoleForAmazonGuardDuty`.

Como excluir manualmente a função vinculada a serviço usando o IAM

Use o console do IAM AWS CLI, o ou a API do IAM para excluir a função `AWSServiceRoleForAmazonGuardDuty` vinculada ao serviço. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Suportado Regiões da AWS

A Amazon GuardDuty oferece suporte ao uso da função `AWSServiceRoleForAmazonGuardDuty` vinculada ao serviço em todos os Regiões da AWS lugares disponíveis GuardDuty . Para obter uma lista das regiões em que GuardDuty está disponível atualmente, consulte os GuardDuty endpoints e cotas da Amazon no. Referência geral da Amazon Web Services

Permissões de função vinculada ao serviço para Proteção contra malware

A Proteção contra malware usa a função vinculada ao serviço (SLR) chamada `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Essa SLR permite que o Malware Protection realize varreduras sem agente para detectar malware em sua conta. GuardDuty Ele permite GuardDuty criar um instantâneo do volume do EBS em sua conta e compartilhar esse instantâneo com a GuardDuty conta de serviço. Depois de GuardDuty avaliar o snapshot, ele inclui os metadados recuperados da instância do EC2 e da carga de trabalho do contêiner nas descobertas da Proteção contra Malware. A função vinculada ao serviço `AWSServiceRoleForAmazonGuardDutyMalwareProtection` confia no serviço `malware-protection.guardduty.amazonaws.com` para presumir a função.

As políticas de permissão para essa função ajudam o Malware Protection a realizar as seguintes tarefas:

- Use as ações do Amazon Elastic Compute Cloud (Amazon EC2) para recuperar informações sobre suas instâncias, volumes e snapshots do Amazon EC2. A Proteção contra malware também fornece permissão para acessar os metadados de clusters do Amazon EKS e do Amazon ECS.
- Crie snapshots para volumes do EBS que tenham a tag `GuardDutyExcluded` não definida como `true`. Por padrão, os snapshots são criados com uma tag `GuardDutyScanId`. Não remova essa tag, caso contrário, a Proteção contra malware não terá acesso aos snapshots.

> **Important**
>
> Quando você define `GuardDutyExcluded` o como`true`, o GuardDuty serviço não poderá acessar esses instantâneos no futuro. Isso ocorre porque as outras instruções nessa

função vinculada ao serviço impedem a execução GuardDuty de qualquer ação nos instantâneos que têm a `GuardDutyExcluded` função definida como. `true`

- Permita o compartilhamento e a exclusão de snapshots somente se a tag `GuardDutyScanId` existir e a tag `GuardDutyExcluded` não estiver definida como `true`.

> **Note**
>
> Não permite que a Proteção contra malware torne os snapshots públicos.

- Acesse as chaves gerenciadas pelo cliente, exceto aquelas que têm uma `GuardDutyExcluded` tag definida como`true`, para ligar `CreateGrant` para criar e acessar um volume criptografado do EBS a partir do snapshot criptografado que é compartilhado com a conta de GuardDuty serviço. Para obter uma lista de contas de GuardDuty serviço para cada região, consulte[GuardDuty contas de serviço por Região da AWS](#).
- Acesse CloudWatch os registros dos clientes para criar o grupo de registros de Proteção contra Malware, bem como colocar os registros de eventos de verificação de malware no `/aws/guardduty/malware-scan-events` grupo de registros.
- Permita que o cliente decida se deseja manter os snapshots nos quais o malware foi detectado em sua conta. Se o escaneamento detectar malware, a função vinculada ao serviço permite adicionar duas tags GuardDuty aos instantâneos - e. `GuardDutyFindingDetected` `GuardDutyExcluded`

> **Note**
>
> A tag `GuardDutyFindingDetected` especifica que os snapshots contêm malware.

- Determine se um volume está criptografado com uma chave gerenciada pelo EBS. GuardDuty executa a `DescribeKey` ação para determinar a `key Id` chave gerenciada pelo EBS em sua conta.
- Obtenha o snapshot dos volumes do EBS criptografados usando Chave gerenciada pela AWS, do seu Conta da AWS e copie-o para o. [GuardDuty conta de serviço](#) Para isso, usamos as permissões `GetSnapshotBlock` `ListSnapshotBlocks` e. GuardDuty em seguida, digitalizará o instantâneo na conta de serviço. Atualmente, o suporte do Malware Protection para escanear volumes do EBS criptografados com Chave gerenciada pela AWS pode não estar disponível em todos os. Regiões da AWS Para ter mais informações, consulte [Disponibilidade de recursos específicos da região](#).

- Permita que o Amazon EC2 ligue AWS KMS em nome da Malware Protection para realizar várias ações criptográficas nas chaves gerenciadas pelo cliente. Ações como `kms:ReEncryptTo` e `kms:ReEncryptFrom` são necessárias para compartilhar os snapshots criptografados com as chaves gerenciadas pelo cliente. Somente as chaves para as quais a tag `GuardDutyExcluded` não está definida como `true` estão acessíveis.

A função é configurada com a seguinte política gerenciada da AWS, denominada `AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "DescribeAndListPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ecs:ListClusters",
                "ecs:ListContainerInstances",
                "ecs:ListTasks",
                "ecs:DescribeTasks",
                "eks:DescribeCluster"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateSnapshotVolumeConditionalStatement",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:*:*:volume/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "CreateSnapshotConditionalStatement",
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshot",
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
```

```
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "GuardDutyScanId"
                }
            }
        },
        {
            "Sid": "CreateTagsPermission",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:*/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSnapshot"
                }
            }
        },
        {
            "Sid": "AddTagsToSnapshotPermission",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GuardDutyScanId": "*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "GuardDutyExcluded",
                        "GuardDutyFindingDetected"
                    ]
                }
            }
        },
        {
            "Sid": "DeleteAndShareSnapshotPermission",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSnapshot",
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
```

```
                    "ec2:ResourceTag/GuardDutyScanId": "*"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        },
        {
            "Sid": "PreventPublicAccessToSnapshotPermission",
            "Effect": "Deny",
            "Action": [
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:Add/group": "all"
                }
            }
        },
        {
            "Sid": "CreateGrantPermission",
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": "arn:aws:kms:*:*:key/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:ebs:id": "snap-*"
                },
                "ForAllValues:StringEquals": {
                    "kms:GrantOperations": [
                        "Decrypt",
                        "CreateGrant",
                        "GenerateDataKeyWithoutPlaintext",
                        "ReEncryptFrom",
                        "ReEncryptTo",
                        "RetireGrant",
                        "DescribeKey"
                    ]
                },
                "Bool": {
```

```
                "kms:GrantIsForAWSResource": "true"
            }
        }
    },
    {
        "Sid": "ShareSnapshotKMSPermission",
        "Effect": "Allow",
        "Action": [
            "kms:ReEncryptTo",
            "kms:ReEncryptFrom"
        ],
        "Resource": "arn:aws:kms:*:*:key/*",
        "Condition": {
            "StringLike": {
                "kms:ViaService": "ec2.*.amazonaws.com"
            },
            "Null": {
                "aws:ResourceTag/GuardDutyExcluded": "true"
            }
        }
    },
    {
        "Sid": "DescribeKeyPermission",
        "Effect": "Allow",
        "Action": "kms:DescribeKey",
        "Resource": "arn:aws:kms:*:*:key/*"
    },
    {
        "Sid": "GuardDutyLogGroupPermission",
        "Effect": "Allow",
        "Action": [
            "logs:DescribeLogGroups",
            "logs:CreateLogGroup",
            "logs:PutRetentionPolicy"
        ],
        "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*"
    },
    {
        "Sid": "GuardDutyLogStreamPermission",
        "Effect": "Allow",
        "Action": [
            "logs:CreateLogStream",
            "logs:PutLogEvents",
            "logs:DescribeLogStreams"
```

```
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/guardduty/*:log-stream:*"
        },
        {
            "Sid": "EBSDirectAPIPermissions",
            "Effect": "Allow",
            "Action": [
                "ebs:GetSnapshotBlock",
                "ebs:ListSnapshotBlocks"
            ],
            "Resource": "arn:aws:ec2:*:*:snapshot/*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/GuardDutyScanId": "*"
                },
                "Null": {
                    "aws:ResourceTag/GuardDutyExcluded": "true"
                }
            }
        }
    ]
}
```

A seguinte política de confiança está anexada à função vinculada a serviço `AWSServiceRoleForAmazonGuardDutyMalwareProtection`:

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

Criar uma função vinculada ao serviço para Proteção contra malware

A função vinculada ao serviço `AWSServiceRoleForAmazonGuardDutyMalwareProtection` é criada automaticamente quando você habilita a Proteção contra Malware pela primeira

vez ou habilita a Proteção contra Malware em uma região com suporte em que ela não tenha sido habilitada anteriormente. Também é possível criar a função vinculada ao serviço `AWSServiceRoleForAmazonGuardDutyMalwareProtection` manualmente usando o console, a CLI ou a API do IAM.

> **Note**
>
> Por padrão, se você for novo na Amazon GuardDuty, a Proteção contra Malware é ativada automaticamente.

> **Important**
>
> A função vinculada ao serviço criada para a conta de GuardDuty administrador delegado não se aplica às contas dos membros. GuardDuty

É necessário configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para que a função `AWSServiceRoleForAmazonGuardDutyMalwareProtection` vinculada ao serviço seja criada com sucesso, a identidade do IAM que você usa GuardDuty deve ter as permissões necessárias. Para conceder as permissões necessárias, anexe a seguinte política ao usuário, grupo ou função do :

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "malware-protection.guardduty.amazonaws.com"
                    ]
```

```
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    ]
}
```

Para obter mais informações sobre como criar a função manualmente, consulte Criar uma função vinculada ao serviço no Guia do usuário do IAM.

Editar uma função vinculada ao serviço para Proteção contra malware

A Proteção contra Malware não permite que você edite a função vinculada a serviço `AWSServiceRoleForAmazonGuardDutyMalwareProtection`. Depois que você criar um perfil vinculado ao serviço, não poderá alterar o nome do perfil, pois várias entidades podem fazer referência ao perfil. No entanto, você poderá 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 para a Proteção contra malware

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 terá uma entidade não utilizada que não seja monitorada ativamente ou mantida.

> **Important**
>
> Você deverá primeiramente desabilitar a Proteção contra Malware em todas as regiões em que estiver habilitada para excluir o `AWSServiceRoleForAmazonGuardDutyMalwareProtection`.
> Se a Proteção contra malware não estiver desabilitada quando você tentar excluir a função vinculada ao serviço, haverá falha na exclusão. Para ter mais informações, consulte Para ativar ou desativar a verificação GuardDuty de malware iniciada.

Quando você escolhe Desabilitar para interromper o serviço de Proteção contra malware, o não `AWSServiceRoleForAmazonGuardDutyMalwareProtection` é excluído automaticamente. Se você escolher Habilitar para iniciar o serviço de Proteção contra Malware novamente, GuardDuty começará a usar o existente`AWSServiceRoleForAmazonGuardDutyMalwareProtection`.

Como excluir manualmente a função vinculada a serviço usando o IAM

Use o console do IAM, a AWS CLI ou a API do IAM para excluir a função vinculada ao `AWSServiceRoleForAmazonGuardDutyMalwareProtection` serviço. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Suportado Regiões da AWS

A Amazon GuardDuty oferece suporte ao uso da função `AWSServiceRoleForAmazonGuardDutyMalwareProtection` vinculada ao serviço em todos os locais em Regiões da AWS que a Proteção contra Malware está disponível.

Para obter uma lista das regiões em que GuardDuty está disponível atualmente, consulte os GuardDuty endpoints e cotas da Amazon no. Referência geral da Amazon Web Services

> **Note**
>
> Atualmente, a Proteção contra Malware não está disponível em AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA).

Solução de problemas de GuardDuty identidade e acesso da Amazon

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com GuardDuty um IAM.

Tópicos

Não estou autorizado a realizar uma ação em GuardDuty

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um recurso *`my-example-widget`* fictício, mas não tem as permissões `guardduty:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 guardduty:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `guardduty:`*`GetWidget`*.

Se você precisar de ajuda, entre em contato com seu administrador da AWS. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam:PassRole.

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

Alguns Serviços da AWS permitem que você passe uma função existente para o serviço, em vez de criar uma nova função de serviço ou função vinculada ao serviço. Para fazê-lo, você deve ter permissões para passar o perfil para o serviço.

O erro do exemplo a seguir ocorre quando uma usuária do IAM de nome `marymajor` tenta usar o console para executar uma ação no GuardDuty. 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 você precisar de ajuda, entre em contato com seu administrador da AWS. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha tenham acesso Conta da AWS aos meus GuardDuty recursos.

Você pode criar uma função que os usuários de outras contas ou pessoas fora da sua organização possam 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 políticas para conceder às pessoas acesso aos seus recursos.

Saiba mais consultando o seguinte:

- Para saber se é GuardDuty compatível com esses recursos, consulteComo a Amazon GuardDuty trabalha com o IAM.
- Saiba como conceder acesso a seus recursos em todos os Contas da AWS pertencentes a você, consulte Fornecendo Acesso a um Usuário do IAM em Outro Conta da AWS Pertencente a Você no Guia de Usuário do IAM.
- Saiba como conceder acesso a seus recursos para terceiros Contas da AWS consultando Fornecendo Acesso a Contas da AWS Pertencentes a Terceiros no Guia do Usuário do IAM.
- Saiba como conceder acesso por meio da federação de identidades consultando Concedendo 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.

AWS políticas gerenciadas para a Amazon GuardDuty

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas AWS gerenciadas do que escrever políticas você mesmo. É necessário tempo e experiência para criar políticas

gerenciadas pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar nossas políticas AWS gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua Conta da AWS. Para obter mais informações sobre políticas AWS gerenciadas, consulte políticas AWS gerenciadas no Guia do usuário do IAM.

AWS os serviços mantêm e atualizam as políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Ocasionalmente, os serviços adicionam permissões adicionais a uma política AWS gerenciada para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e perfis) em que a política está anexada. É mais provável que os serviços atualizem uma política AWS gerenciada quando um novo recurso é lançado ou quando novas operações são disponibilizadas. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violarão suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política ReadOnlyAccess AWS gerenciada fornece acesso somente de leitura a todos os AWS serviços e recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de perfis de trabalho, consulte Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.

AWS política gerenciada: AmazonGuardDutyFullAccess

É possível anexar a política `AmazonGuardDutyFullAccess` a suas identidades do IAM.

Essa política concede permissões administrativas que permitem ao usuário acesso total a todas as GuardDuty ações.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `GuardDuty`— Permite aos usuários acesso total a todas as GuardDuty ações.
- `IAM`— Permite que os usuários criem a função GuardDuty vinculada ao serviço. Isso permite que um GuardDuty administrador habilite contas GuardDuty de membros.
- `Organizations`— Permite que os usuários designem um administrador delegado e gerenciem os membros de uma GuardDuty organização.

A permissão para realizar uma ação `iam:GetRole` no `AWSServiceRoleForAmazonGuardDutyMalwareProtection` estabelece se a função vinculada ao serviço (SLR) da Proteção contra malware existe em uma conta.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonGuardDutyFullAccessSid1",
            "Effect": "Allow",
            "Action": "guardduty:*",
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoleSid1",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": [
                        "guardduty.amazonaws.com",
                        "malware-protection.guardduty.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "ActionsForOrganizationsSid1",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "IamGetRoleSid1",
            "Effect": "Allow",
            "Action": "iam:GetRole",
            "Resource": "arn:aws:iam::*:role/
*AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    ]
}
```

AWS política gerenciada: AmazonGuardDutyReadOnlyAccess

É possível anexar a política `AmazonGuardDutyReadOnlyAccess` a suas identidades do IAM.

Essa política concede permissões somente para leitura que permitem ao usuário visualizar GuardDuty descobertas e detalhes da sua GuardDuty organização.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `GuardDuty`— Permite que os usuários visualizem GuardDuty as descobertas e realizem operações de API que comecem com `GetList`, ou`Describe`.
- `Organizations`— permite que os usuários recuperem informações sobre a configuração GuardDuty da sua organização, incluindo detalhes da conta do administrador delegado.

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

```
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS política gerenciada: AmazonGuardDutyServiceRolePolicy

Não é possível anexar `AmazonGuardDutyServiceRolePolicy` às entidades do IAM. Essa política AWS gerenciada é anexada a uma função vinculada ao serviço que permite GuardDuty realizar ações em seu nome. Para ter mais informações, consulte Permissões de função vinculadas ao serviço para GuardDuty.

GuardDuty atualizações nas políticas AWS gerenciadas

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

Alteração	Descrição	Data
AmazonGuardDutyServiceRolePolicy - Atualizar para uma política existente	Use AWS Systems Manager ações para gerenciar associações de SSM em instâncias do Amazon EC2 ao GuardDuty habilitar o Runtime Monitoring com agente automatizado para o Amazon EC2. Quando a configuração GuardDuty automatizada do agente está desativada, GuardDuty considera	26 de março de 2024

Alteração	Descrição	Data
	somente as instâncias do EC2 que têm uma tag de inclusão (`GuardDuty Managed :true`).	
AmazonGuardDutyServiceRolePolicy: atualizar para uma política existente.	GuardDuty adicionou uma nova permissão: `organization:DescribeOrganization` recuperar o ID da organização da conta compartilhada da Amazon VPC e definir a política de endpoint do Amazon VPC com o ID da organização.	9 de fevereiro de 2024
AmazonGuardDutyMalwareProtectionServiceRolePolítica — Atualização de uma política existente.	A Proteção contra Malware adicionou duas permissões: obter o instantâneo de um volume do EBS (usando criptografia Chave gerenciada pela AWS) do seu Conta da AWS e copiá-lo para a conta de GuardDuty serviço antes de iniciar a verificação de malware. `GetSnapshotBlock ListSnapshotBlocks`	25 de janeiro de 2024

Alteração	Descrição	Data
AmazonGuardDutyServiceRolePolicy: atualização para uma política existente	Foram adicionadas novas permissões GuardDuty para permitir adicionar configurações de conta do `guardduty Activate` Amazon ECS e realizar operações de lista e descrição nos clusters do Amazon ECS.	26 de novembro de 2023
AmazonGuardDutyReadOnlyAccess: atualização para uma política existente	GuardDuty adicionou uma nova política `organizations` para `ListAccounts`o.	16 de novembro de 2023
AmazonGuardDutyFullAccess: atualização para uma política existente	GuardDuty adicionou uma nova política `organizations` para `ListAccounts`o.	16 de novembro de 2023
AmazonGuardDutyServiceRolePolicy: atualização para uma política existente	GuardDuty adicionou novas permissões para oferecer suporte ao próximo recurso de monitoramento de tempo de execução do GuardDuty EKS.	8 de março de 2023

Alteração	Descrição	Data
AmazonGuardDutyServiceRolePolicy: atualização para uma política existente	GuardDuty adicionou novas permissões para permitir GuardDuty a criação de uma função vinculada ao serviço para proteção contra malware. Isso ajudará a GuardDuty agilizar o processo de ativação da Proteção contra Malware. GuardDuty agora pode realizar a seguinte ação do IAM: `{ "Effect": "Allow", "Action": "iam:CreateServiceLinkedRole", "Resource": "*", "Condition": { "StringEquals": { "iam:AWSServiceName": "malware-protection.guardduty.amazonaws.com" } } }`	21 de fevereiro de 2023
AmazonGuardDutyFullAccess: atualização para uma política existente	GuardDuty ARN atualizado para `iam:GetRole . *AWSServiceRoleForAmazonGuardDutyMalwareProtection`	26 de julho de 2022

Alteração	Descrição	Data
AmazonGuardDutyFullAccess: atualização para uma política existente	GuardDuty adicionou uma nova `AWSServiceName` para permitir a criação de uma função vinculada ao serviço usando o serviço `iam:CreateServiceLinkedRole` de Proteção contra GuardDuty Malware. GuardDuty agora pode realizar a `iam:GetRole` ação para obter informaçõ esAWSServiceRole .	26 de julho de 2022

Alteração	Descrição	Data
AmazonGuardDutyServiceRolePolicy: atualização para uma política existente	GuardDuty adicionou novas permissões GuardDuty para permitir o uso das ações de rede do Amazon EC2 para melhorar as descobertas. GuardDuty agora você pode realizar as seguintes ações do EC2 para obter informações sobre como suas instâncias do EC2 estão se comunicando. Essas informações são usadas para melhorar a precisão da descoberta. • `ec2:DescribeVpcEndpoints` • `ec2:DescribeSubnets` • `ec2:DescribeVpcPeeringConnections` • `ec2:DescribeTransitGatewayAttachments`	3 de agosto de 2021
GuardDuty começou a rastrear as alterações	GuardDuty começou a rastrear as mudanças em suas políticas AWS gerenciadas.	3 de agosto de 2021

Validação de conformidade para a Amazon GuardDuty

Para saber se um AWS service (Serviço da AWS) está no escopo de programas de conformidade específicos, consulte Serviços da AWS em Escopo por Programa de Conformidade e escolha o

programa de conformidade no qual estiver interessado. Para obter informações gerais, consulte AWSProgramas de Conformidade.

Você pode fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Fazer Download de Relatório em AWS Artifact.

Sua responsabilidade de conformidade ao usar o Serviços da AWS é determinada pela sensibilidade dos seus dados, pelos objetivos de conformidade da sua empresa, pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes recursos para ajudar com a conformidade:

- Guias de Início Rápido de Segurança e Conformidade –- estes guias de implantação debatem considerações sobre arquitetura e fornecem as etapas para a implantação de ambientes de linha de base focados em segurança e conformidade na AWS.
- Arquitetura para segurança e conformidade com HIPAA no Amazon Web Services: esse whitepaper descreve como as empresas podem usar a AWS para criar aplicações adequadas aos padrões HIPAA.

  > **Note**
  >
  > Nem todos os Serviços da AWS estão qualificados pela HIPAA. Para obter mais informações, consulte Referência dos Serviços Qualificados pela HIPAA.

- AWSRecursos de Conformidade da –- essa coleção de manuais e guias pode ser aplicada ao seu setor e local.
- Guias de conformidade do cliente da AWS: entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as práticas recomendadas para proteção de Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliar recursos com regras no Guia do desenvolvedor do AWS Config : o serviço AWS Config avalia como as configurações de recursos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub –- este AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança na AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do

setor de segurança. Para obter uma lista dos serviços com suporte e controles aceitos, consulte a Referência de controles do Security Hub.

- AWS Audit Manager: esse AWS service (Serviço da AWS) ajuda a auditar continuamente seu uso da AWS para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

Resiliência no Amazon GuardDuty

A infraestrutura global da AWS é criada com base em regiões e zonas de disponibilidade da AWS. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, alta throughput e redes altamente redundantes. 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 data center tradicionais.

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

Segurança da infraestrutura no Amazon GuardDuty

Como um serviço gerenciado, o Amazon GuardDuty é protegido pela segurança da rede global da AWS. Para obter informações sobre serviços de segurança da AWS e como a AWS protege a infraestrutura, consulte Segurança na Nuvem AWS. Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança de infraestrutura, consulte Proteção de infraestrutura em Pilar segurança: AWS Well-Architected Framework.

Você usa chamadas de API publicadas pela AWS para acessar o GuardDuty 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 perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS

Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Integrações de serviços da AWS com o GuardDuty

O GuardDuty pode ser integrado a outros serviços de segurança da AWS. Esses serviços podem ingerir dados do GuardDuty para permitir que você visualize as descobertas de novas maneiras. Veja as opções de integração a seguir para saber mais sobre como cada serviço é configurado para funcionar com o GuardDuty.

Integração do GuardDuty com o AWS Security Hub

O AWS Security Hub coleta dados de segurança das contas da AWS, serviços e produtos compatíveis de terceiros parceiros para avaliar o estado de segurança do seu ambiente de acordo com os padrões do setor e as práticas recomendadas. Além de avaliar sua postura de segurança, o Security Hub cria um local central para descobertas em todos os seus serviços integrados da AWS e produtos de parceiros da AWS. Habilitar o Security Hub com o GuardDuty permitirá automaticamente que os dados de descobertas do GuardDuty sejam ingeridos pelo Security Hub.

Para obter mais informações sobre como usar o Security Hub com o GuardDuty, consulte Integração com AWS Security Hub.

Integração do GuardDuty com o Amazon Detective

O Amazon Detective usa dados de log de todas as suas contas da AWS para criar visualizações de dados para seus recursos e endereços IP que interagem com seu ambiente. As visualizações do Detective ajudam você a investigar problemas de segurança com rapidez e facilidade. Você pode passar de detalhes de descobertas do GuardDuty para as informações no console do Detective quando os dois serviços estiverem habilitados.

Para obter mais informações sobre como usar o Detective com o GuardDuty, consulte Integração com o Amazon Detective.

Integração com AWS Security Hub

O AWS Security Hub fornece uma visão abrangente do estado de segurança na AWS e ajuda a verificar o ambiente em relação aos padrões e às práticas recomendadas do setor de segurança. O Security Hub coleta dados de segurança de várias AWS contas, serviços e produtos de parceiros terceirizados compatíveis e ajuda você a analisar suas tendências de segurança e identificar os problemas de segurança de maior prioridade.

A GuardDuty integração da Amazon com o Security Hub permite que você envie descobertas GuardDuty para o Security Hub. O Security Hub pode então incluir tais descobertas na análise feita sobre a seu procedimento de segurança.

Sumário

Como a Amazon GuardDuty envia descobertas para AWS Security Hub

Em AWS Security Hub, os problemas de segurança são rastreados como descobertas. Algumas descobertas vêm de problemas detectados por outros AWS serviços ou por parceiros terceirizados. O Security Hub também tem um conjunto de regras que ele usa para detectar problemas de segurança e gerar descobertas.

O Security Hub fornece ferramentas para gerenciar descobertas em todas essas fontes. Você pode exibir e filtrar listas de descobertas e exibir detalhes de uma descoberta. Para obter mais informações, consulte Visualizar descobertas no Guia do usuário do AWS Security Hub . Você também pode rastrear o status de uma investigação em uma descoberta. Para obter mais informações, consulte Tomar medidas sobre descobertas no Manual do usuário do AWS Security Hub .

Todas as descobertas no Security Hub usam um formato JSON padrão chamado AWS Security Finding Format (ASFF). O ASFF inclui detalhes sobre a origem do problema, os recursos afetados e o status atual da descoberta. Consulte ASFF (Formato de Descoberta de Segurança) da AWS no Guia do usuário do AWS Security Hub .

A Amazon GuardDuty é um dos AWS serviços que envia descobertas para o Security Hub.

Tipos de descobertas GuardDuty enviadas ao Security Hub

Depois de ativar o GuardDuty Security Hub na mesma conta dentro da mesma Região da AWS, GuardDuty começa a enviar todas as descobertas geradas para o Security Hub. Essas descobertas são enviadas ao Security Hub usando o AWS Security Finding Format (ASFF). No ASFF, o campo `Types` fornece o tipo de descoberta.

Latência para envio de novas descobertas

Quando GuardDuty cria uma nova descoberta, ela geralmente é enviada ao Security Hub em cinco minutos.

Tentar novamente quando o Security Hub não estiver disponível

Se o Security Hub não estiver disponível, GuardDuty tente enviar novamente as descobertas até que elas sejam recebidas.

Atualizar as descobertas do existentes no Security Hub

Depois de enviar uma descoberta para o Security Hub, GuardDuty envia atualizações para refletir observações adicionais da atividade de descoberta para o Security Hub. As novas observações dessas descobertas são enviadas ao Security Hub com base nas Etapa 5 — Exportar frequência de atualização configurações do seu Conta da AWS.

Quando você arquiva ou desarquiva uma descoberta, GuardDuty não a envia para o Security Hub. Qualquer descoberta desarquivada manualmente que posteriormente se torne ativa não GuardDuty é enviada para o Security Hub.

Visualizando GuardDuty descobertas em AWS Security Hub

Para ver suas GuardDuty descobertas no Security Hub, selecione Ver descobertas na Amazon na página GuardDuty de resumo. Como alternativa, você pode selecionar Descobertas no painel de navegação e filtrar as descobertas para exibir somente GuardDuty as descobertas selecionando o campo Nome do produto: com um valor de`GuardDuty`.

Interpretando GuardDuty encontrar nomes em AWS Security Hub

GuardDuty envia as descobertas para o Security Hub usando o AWS Security Finding Format (ASFF). No ASFF, o campo `Types` fornece o tipo de descoberta. Os tipos ASFF usam um esquema

de nomenclatura diferente dos tipos. GuardDuty A tabela abaixo detalha todos os tipos de GuardDuty descobertas com seus equivalentes do ASFF conforme aparecem no Security Hub.

> **Note**
>
> Para alguns tipos de GuardDuty descoberta, o Security Hub atribui nomes de descoberta ASFF diferentes, dependendo se a função de recurso do detalhe da descoberta era ACTOR ou TARGET. Para obter mais informações, consulte Detalhes da descoberta.

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Backdoor:EC2/C&CActivity.B	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B
Backdoor:EC2/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:EC2-C&CActivity.B!DNS
Backdoor:EC2/DenialOfService.Dns	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Dns
Backdoor:EC2/DenialOfService.Tcp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Tcp
Backdoor:EC2/DenialOfService.Udp	TTPs/Command and Control/Backdoor:EC2-DenialOfService.Udp
Backdoor:EC2/DenialOfService.UdpOnTcpPorts	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UdpOnTcpPorts
Backdoor:EC2/DenialOfService.UnusualProtocol	TTPs/Command and Control/Backdoor:EC2-DenialOfService.UnusualProtocol
Backdoor:EC2/Spambot	TTPs/Command and Control/Backdoor:EC2-Spambot
Behavior:EC2/NetworkPortUnusual	Unusual Behaviors/VM/Behavior:EC2-NetworkPortUnusual

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Behavior:EC2/TrafficVolumeUnusual	Unusual Behaviors/VM/Behavior:EC2-TrafficVolumeUnusual
Backdoor:Lambda/C&CActivity.B	TTPs/Command and Control/Backdoor:Lambda-C&CActivity.B
Backdoor:Runtime/C&CActivity.B	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B
Backdoor:Runtime/C&CActivity.B!DNS	TTPs/Command and Control/Backdoor:Runtime-C&CActivity.B!DNS
CredentialAccess:IAMUser/AnomalousBehavior	TTPs/Credential Access/IAMUser-AnomalousBehavior
CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed	TTPs/AnomalousBehavior/CredentialAccess:Kubernetes-SecretsAccessed
CredentialAccess:RDS/AnomalousBehavior.FailedLogin	TTPs/Credential Access/CredentialAccess:RDS-AnomalousBehavior.FailedLogin
CredentialAccess:RDS/AnomalousBehavior.SuccessfulBruteForce	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulBruteForce
CredentialAccess:RDS/AnomalousBehavior.SuccessfulLogin	TTPs/Credential Access/RDS-AnomalousBehavior.SuccessfulLogin
CredentialAccess:RDS/MaliciousIPCaller.FailedLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.FailedLogin
CredentialAccess:RDS/MaliciousIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-MaliciousIPCaller.SuccessfulLogin
CredentialAccess:RDS/TorIPCaller.FailedLogin	TTPs/Credential Access/RDS-TorIPCaller.FailedLogin
CredentialAccess:RDS/TorIPCaller.SuccessfulLogin	TTPs/Credential Access/RDS-TorIPCaller.SuccessfulLogin

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
CryptoCurrency:EC2/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B
CryptoCurrency:EC2/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:EC2-BitcoinTool.B!DNS
CryptoCurrency:Lambda/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Lambda-BitcoinTool.B Effects/Resource Consumption/CryptoCurrency:Lambda-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B
CryptoCurrency:Runtime/BitcoinTool.B!DNS	TTPs/Command and Control/CryptoCurrency:Runtime-BitcoinTool.B!DNS
DefenseEvasion:EC2/UnusualDNSResolver	TTPs/DefenseEvasion/EC2:Unusual-DNS-Resolver
DefenseEvasion:EC2/UnusualDoHActivity	TTPs/DefenseEvasion/EC2:Unusual-DoH-Activity
DefenseEvasion:EC2/UnusualDoTActivity	TTPs/DefenseEvasion/EC2:Unusual-DoT-Activity
DefenseEvasion:Sou usuário/ Anomalous Behavior	TTPs/Defense Evasion/IAMUser-AnomalousBehavior
DefenseEvasion:Runtime/FilelessExecution	TTPs/Defense Evasion/DefenseEvasion:Runtime-FilelessExecution
DefenseEvasion:Runtime/PtraceAntiDebugging	TTPs/DefenseEvasion/DefenseEvasion:Runtime-PtraceAntiDebugging
DefenseEvasion:Runtime/SuspiciousCommand	TTPs/DefenseEvasion/DefenseEvasion:Runtime-SuspiciousCommand

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Descoberta: eu sou usuário/ Anomalous Behavior	TTPs/Discovery/IAMUser-AnomalousBehavior
Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	TTPs/AnomalousBehavior/Discovery:Kubernetes-PermissionChecked
Discovery:RDS/MaliciousIPCaller	TTPs/Discovery/RDS-MaliciousIPCaller
Discovery:RDS/TorIPCaller	TTPs/Discovery/RDS-TorIPCaller
Discovery:S3/AnomalousBehavior	TTPs/Discovery:S3-AnomalousBehavior
Discovery:S3/BucketEnumeration.Unusual	TTPs/Discovery:S3-BucketEnumeration.Unusual
Discovery:S3/MaliciousIPCaller.Custom	TTPs/Discovery:S3-MaliciousIPCaller.Custom
Discovery:S3/TorIPCaller	TTPs/Discovery:S3-TorIPCaller
Discovery:S3/MaliciousIPCaller	TTPs/Discovery:S3-MaliciousIPCaller
Execution:Kubernetes/AnomalousBehavior.ExecInPod	TTPs/AnomalousBehavior/Execution:Kubernetes-ExecInPod
Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	TTPs/AnomalousBehavior/Execution:Kubernetes-WorkloadDeployed
Persistence:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount	TTPs/AnomalousBehavior/Persistence:Kubernetes-WorkloadDeployed!ContainerWithSensitiveMount
PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer	TTPs/AnomalousBehavior/PrivilegeEscalation:Kubernetes-WorkloadDeployed!PrivilegedContainer
Execution:EC2/MaliciousFile	TTPs/Execution/Execution:EC2-MaliciousFile
Execution:ECS/MaliciousFile	TTPs/Execution/Execution:ECS-MaliciousFile

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Execution:Kubernetes/MaliciousFile	TTPs/Execution/Execution:Kubernetes-MaliciousFile
Execution:Container/MaliciousFile	TTPs/Execution/Execution:Container-MaliciousFile
Execution:EC2/SuspiciousFile	TTPs/Execution/Execution:EC2-SuspiciousFile
Execution:ECS/SuspiciousFile	TTPs/Execution/Execution:ECS-SuspiciousFile
Execution:Kubernetes/SuspiciousFile	TTPs/Execution/Execution:Kubernetes-SuspiciousFile
Execution:Container/SuspiciousFile	TTPs/Execution/Execution:Container-SuspiciousFile
Execution:Runtime/MaliciousFileExecuted	TTPs/Execution/Execution:Runtime-MaliciousFileExecuted
Execution:Runtime/NewBinaryExecuted	TTPs/Execution/Execution:Runtime-NewBinaryExecuted
Execution:Runtime/NewLibraryLoaded	TTPs/Execution/Execution:Runtime-NewLibraryLoaded
Execution:Runtime/ReverseShell	TTPs/Execution/Execution:Runtime-ReverseShell
Execution:Runtime/SuspiciousCommand	TTPs/Execution/Execution:Runtime-SuspiciousCommand
Execution:Runtime/SuspiciousTool	TTPs/Execution/Execution:Runtime-SuspiciousTool
Exfiltration:S3/AnomalousBehavior	TTPs/Exfiltration:S3-AnomalousBehavior
Exfiltration:S3/ObjectRead.Unusual	TTPs/Exfiltration:S3-ObjectRead.Unusual

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Exfiltration:S3/MaliciousIPCaller	TTPs/Exfiltration:S3-MaliciousIPCaller
Impact:EC2/AbusedDomainRequest.Reputation	TTPs/Impact:EC2-AbusedDomainRequest.Reputation
Impact:EC2/BitcoinDomainRequest.Reputation	TTPs/Impact:EC2-BitcoinDomainRequest.Reputation
Impact:EC2/MaliciousDomainRequest.Reputation	TTPs/Impact:EC2-MaliciousDomainRequest.Reputation
Impact:EC2/PortSweep	TTPs/Impact/Impact:EC2-PortSweep
Impact:EC2/SuspiciousDomainRequest.Reputation	TTPs/Impact:EC2-SuspiciousDomainRequest.Reputation
Impact:EC2/WinRMBruteForce	TTPs/Impact/Impact:EC2-WinRMBruteForce
Impacto: iamUser/ AnomalousBehavior	TTPs/Impact/IAMUser-AnomalousBehavior
Impact:Runtime/AbusedDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-AbusedDomainRequest.Reputation
Impact:Runtime/BitcoinDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-BitcoinDomainRequest.Reputation
Impact:Runtime/CryptoMinerExecuted	TTPs/Impact/Impact:Runtime-CryptoMinerExecuted
Impact:Runtime/MaliciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation
Impact:Runtime/SuspiciousDomainRequest.Reputation	TTPs/Impact/Impact:Runtime-SuspiciousDomainRequest.Reputatio
Impact:S3/AnomalousBehavior.Delete	TTPs/Impact:S3-AnomalousBehavior.Delete

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Impact:S3/AnomalousBehavior.Permission	TTPs/Impact:S3-AnomalousBehavior.Permission
Impact:S3/AnomalousBehavior.Write	TTPs/Impact:S3-AnomalousBehavior.Write
Impact:S3/ObjectDelete.Unusual	TTPs/Impact:S3-ObjectDelete.Unusual
Impact:S3/PermissionsModification.Unusual	TTPs/Impact:S3-PermissionsModification.Unusual
Impact:S3/MaliciousIPCaller	TTPs/Impact:S3-MaliciousIPCaller
InitialAccess:Sou usuário/ AnomalousBehavior	TTPs/Initial Access/IAMUser-AnomalousBehavior
PenTest:IAMUser/KaliLinux	TTPs/PenTest:IAMUser/KaliLinux
PenTest:IAMUser/ParrotLinux	TTPs/PenTest:IAMUser/ParrotLinux
PenTest:IAMUser/PentooLinux	TTPs/PenTest:IAMUser/PentooLinux
PenTest:S3/KaliLinux	TTPs/PenTest:S3-KaliLinux
PenTest:S3/ParrotLinux	TTPs/PenTest:S3-ParrotLinux
PenTest:S3/PentooLinux	TTPs/PenTest:S3-PentooLinux
Persistência: iamuser/ AnomalousBehavior	TTPs/Persistence/IAMUser-AnomalousBehavior
Persistence:IAMUser/NetworkPermissions	TTPs/Persistence/Persistence:IAMUser-NetworkPermissions
Persistence:IAMUser/ResourcePermissions	TTPs/Persistence/Persistence:IAMUser-ResourcePermissions
Persistence:IAMUser/UserPermissions	TTPs/Persistence/Persistence:IAMUser-UserPermissions

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Policy:IAMUser/RootCredentialUsage	TTPs/Policy:IAMUser-RootCredentialUsage
Policy:S3/AccountBlockPublicAccessDisabled	TTPs/Policy:S3-AccountBlockPublicAccessDisabled
Policy:S3/BucketAnonymousAccessGranted	TTPs/Policy:S3-BucketAnonymousAccessGranted
Policy:S3/BucketBlockPublicAccessDisabled	Effects/Data Exposure/Policy:S3-BucketBlockPublicAccessDisabled
Policy:S3/BucketPublicAccessGranted	TTPs/Policy:S3-BucketPublicAccessGranted
PrivilegeEscalation:Sou usuário/ AnomalousBehavior	TTPs/Privilege Escalation/IAMUser-AnomalousBehavior
PrivilegeEscalation:IAMUser/AdministrativePermissions	TTPs/Privilege Escalation/PrivilegeEscalation:IAMUser-AdministrativePermissions
PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated	TTPs/AnomalousBehavior/PriviledgeEscalation:Kubernetes-RoleBindingCreated
PriviledgeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	TTPs/AnomalousBehavior/PriviledgeEscalation:Kubernetes-RoleCreated
PrivilegeEscalation:Runtime/ContainerMountsHostDirectory	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-ContainerMountsHostDirectory
PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-CGroupsReleaseAgentModified
PrivilegeEscalation:Runtime/DockerSocketAccessed	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-DockerSocketAccessed
PrivilegeEscalation:Runtime/RuncContainerEscape	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-RuncContainerEscape

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
PrivilegeEscalation:Runtime/UserfaultfdUsage	TTPs/Privilege Escalation/PrivilegeEscalation:Runtime-UserfaultfdUsage
Recon:EC2/PortProbeEMRUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeEMRUnprotectedPort
Recon:EC2/PortProbeUnprotectedPort	TTPs/Discovery/Recon:EC2-PortProbeUnprotectedPort
Recon:EC2/Portscan	TTPs/Discovery/Recon:EC2-Portscan
Recon:IAMUser/MaliciousIPCaller	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller
Recon:IAMUser/MaliciousIPCaller.Custom	TTPs/Discovery/Recon:IAMUser-MaliciousIPCaller.Custom
Recon:IAMUser/NetworkPermissions	TTPs/Discovery/Recon:IAMUser-NetworkPermissions
Recon:IAMUser/ResourcePermissions	TTPs/Discovery/Recon:IAMUser-ResourcePermissions
Recon:IAMUser/TorIPCaller	TTPs/Discovery/Recon:IAMUser-TorIPCaller
Recon:IAMUser/UserPermissions	TTPs/Discovery/Recon:IAMUser-UserPermissions
ResourceConsumption:IAMUser/ComputeResources	Unusual Behaviors/User/ResourceConsumption:IAMUser-ComputeResources
Stealth:IAMUser/CloudTrailLoggingDisabled	TTPs/Defense Evasion/Stealth:IAMUser-CloudTrailLoggingDisabled
Stealth:IAMUser/LoggingConfigurationModified	TTPs/Defense Evasion/Stealth:IAMUser-LoggingConfigurationModified

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Stealth:IAMUser/PasswordPolicyChange	TTPs/Defense Evasion/Stealth:IAMUser-PasswordPolicyChange
Stealth:S3/ServerAccessLoggingDisabled	TTPs/Defense Evasion/Stealth:S3-ServerAccessLoggingDisabled
Trojan:EC2/BlackholeTraffic	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic
Trojan:EC2/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:EC2-BlackholeTraffic!DNS
Trojan:EC2/DGADomainRequest.B	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.B
Trojan:EC2/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:EC2-DGADomainRequest.C!DNS
Trojan:EC2/DNSDataExfiltration	TTPs/Command and Control/Trojan:EC2-DNSDataExfiltration
Trojan:EC2/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:EC2-DriveBySourceTraffic!DNS
Trojan:EC2/DropPoint	Effects/Data Exfiltration/Trojan:EC2-DropPoint
Trojan:EC2/DropPoint!DNS	Effects/Data Exfiltration/Trojan:EC2-DropPoint!DNS
Trojan:EC2/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:EC2-PhishingDomainRequest!DNS
Trojan:Lambda/BlackholeTraffic	TTPs/Command and Control/Trojan:Lambda-BlackholeTraffic
Trojan:Lambda/DropPoint	Effects/Data Exfiltration/Trojan:Lambda-DropPoint

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
Trojan:Runtime/BlackholeTraffic	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic
Trojan:Runtime/BlackholeTraffic!DNS	TTPs/Command and Control/Trojan:Runtime-BlackholeTraffic!DNS
Trojan:Runtime/DGADomainRequest.C!DNS	TTPs/Command and Control/Trojan:Runtime-DGADomainRequest.C!DNS
Trojan:Runtime/DriveBySourceTraffic!DNS	TTPs/Initial Access/Trojan:Runtime-DriveBySourceTraffic!DNS
Trojan:Runtime/DropPoint	Effects/Data Exfiltration/Trojan:Runtime-DropPoint
Trojan:Runtime/DropPoint!DNS	Effects/Data Exfiltration/Trojan:Runtime-DropPoint!DNS
Trojan:Runtime/PhishingDomainRequest!DNS	TTPs/Command and Control/Trojan:Runtime-PhishingDomainRequest!DNS
UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:EC2-MaliciousIPCaller.Custom
UnauthorizedAccess:EC2/MetadataDNSRebind	TTPs/UnauthorizedAccess:EC2-MetadataDNSRebind
UnauthorizedAccess:EC2/RDPBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-RDPBruteForce
UnauthorizedAccess:EC2/SSHBruteForce	TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce
UnauthorizedAccess:EC2/TorClient	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorClient
UnauthorizedAccess:EC2/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:EC2-TorRelay

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
UnauthorizedAccess:IAMUser/ConsoleLogin	Unusual Behaviors/User/Unauthorized Access:IAMUser-ConsoleLogin
UnauthorizedAccess:IAMUser/ConsoleLoginSuccess.B	TTPs/UnauthorizedAccess:IAMUser-ConsoleLoginSuccess.B
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.InsideAWS
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	Effects/Data Exfiltration/UnauthorizedAccess:IAMUser-InstanceCredentialExfiltration.OutsideAWS
UnauthorizedAccess:IAMUser/MaliciousIPCaller	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller
UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:IAMUser-MaliciousIPCaller.Custom
UnauthorizedAccess:IAMUser/TorIPCaller	TTPs/Command and Control/UnauthorizedAccess:IAMUser-TorIPCaller
UnauthorizedAccess:Lambda/MaliciousIPCaller.Custom	TTPs/Command and Control/UnauthorizedAccess:Lambda-MaliciousIPCaller.Custom
UnauthorizedAccess:Lambda/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorClient
UnauthorizedAccess:Lambda/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Lambda-TorRelay
UnauthorizedAccess:Runtime/MetadataDNSRebind	TTPs/UnauthorizedAccess:Runtime-MetadataDNSRebind
UnauthorizedAccess:Runtime/TorRelay	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorRelay

GuardDuty tipo de descoberta	Tipo de descoberta do ASFF
UnauthorizedAccess:Runtime/TorClient	Effects/Resource Consumption/UnauthorizedAccess:Runtime-TorClient
UnauthorizedAccess:S3/MaliciousIPCaller.Custom	TTPs/UnauthorizedAccess:S3-MaliciousIPCaller.Custom
UnauthorizedAccess:S3/TorIPCaller	TTPs/UnauthorizedAccess:S3-TorIPCaller

Descoberta típica do GuardDuty

GuardDuty envia descobertas para o Security Hub usando o AWS Security Finding Format (ASFF).

Aqui está um exemplo de uma descoberta típica de GuardDuty.


```
  {
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductArn": "arn:aws::securityhub:us-east-1:product/aws/guardduty",
  "GeneratorId": "arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64",
  "AwsAccountId": "193043430472",
  "Types": [
    "TTPs/Initial Access/UnauthorizedAccess:EC2-SSHBruteForce"
  ],
  "FirstObservedAt": "2020-08-22T09:15:57Z",
  "LastObservedAt": "2020-09-30T11:56:49Z",
  "CreatedAt": "2020-08-22T09:34:34.146Z",
  "UpdatedAt": "2020-09-30T12:14:00.206Z",
  "Severity": {
    "Product": 2,
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356.",
  "Description": "199.241.229.197 is performing SSH brute force attacks against
 i-0c10c2c7863d1a356. Brute force attacks are used to gain unauthorized access to your
 instance by guessing the SSH password.",
```

```
  "SourceUrl": "https://us-east-1.console.aws.amazon.com/guardduty/home?region=us-
east-1#/findings?macros=current&fId=46ba0ac2845071e23ccdeb2ae03bfdea",
  "ProductFields": {
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/portName":
 "Unknown",
    "aws/guardduty/service/archived": "false",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asnOrg": "CENTURYLINK-US-LEGACY-QWEST",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lat": "42.5122",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/ipAddressV4":
 "199.241.229.197",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/geoLocation/
lon": "-90.7384",
    "aws/guardduty/service/action/networkConnectionAction/blocked": "false",
    "aws/guardduty/service/action/networkConnectionAction/remotePortDetails/port":
 "46717",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/country/
countryName": "United States",
    "aws/guardduty/service/serviceName": "guardduty",
    "aws/guardduty/service/evidence": "",
    "aws/guardduty/service/action/networkConnectionAction/localIpDetails/ipAddressV4":
 "172.31.43.6",
    "aws/guardduty/service/detectorId": "d4b040365221be2b54a6264dc9a4bc64",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
org": "CenturyLink",
    "aws/guardduty/service/action/networkConnectionAction/connectionDirection":
 "INBOUND",
    "aws/guardduty/service/eventFirstSeen": "2020-08-22T09:15:57Z",
    "aws/guardduty/service/eventLastSeen": "2020-09-30T11:56:49Z",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/portName":
 "SSH",
    "aws/guardduty/service/action/actionType": "NETWORK_CONNECTION",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/city/
cityName": "Dubuque",
    "aws/guardduty/service/additionalInfo": "",
    "aws/guardduty/service/resourceRole": "TARGET",
    "aws/guardduty/service/action/networkConnectionAction/localPortDetails/port": "22",
    "aws/guardduty/service/action/networkConnectionAction/protocol": "TCP",
    "aws/guardduty/service/count": "74",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
asn": "209",
    "aws/guardduty/service/action/networkConnectionAction/remoteIpDetails/organization/
isp": "CenturyLink",
```

```
    "aws/securityhub/FindingId": "arn:aws::securityhub:us-east-1::product/
aws/guardduty/arn:aws::guardduty:us-east-1:193043430472:detector/
d4b040365221be2b54a6264dc9a4bc64/finding/46ba0ac2845071e23ccdeb2ae03bfdea",
    "aws/securityhub/ProductName": "GuardDuty",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws::ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
          "Type": "t2.micro",
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "18.234.130.16",
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475",
          "LaunchedAt": "2020-08-03T23:21:57Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```


Habilitar e configurar a integração

Para usar a integração com AWS Security Hub, você deve habilitar o Security Hub. Para obter informações sobre como habilitar o Security Hub, consulte Configurar o Security Hub no Guia do usuário AWS Security Hub .

Quando você ativa o Security Hub GuardDuty e o Security Hub, a integração é ativada automaticamente. GuardDutyimediatamente começa a enviar as descobertas para o Security Hub.

Como interromper a publicação de descobertas no Security Hub

Para interromper o envio das descobertas ao Security Hub, você poderá usar o console ou a API do Security Hub.

Consulte Desabilitar e habilitar o fluxo de descobertas de uma integração (console) ou Desabilitar o fluxo de descobertas de uma integração (API do Security Hub, AWS CLI) no Guia do Usuário.AWS Security Hub

Integração com o Amazon Detective

O Amazon Detective ajuda você a analisar e investigar rapidamente eventos de segurança em uma ou mais contas da AWS, gerando visualizações de dados que representam a forma como seus recursos se comportam e interagem ao longo do tempo. Detective cria visualizações das descobertas do GuardDuty.

Detective ingere detalhes de descoberta para todos os tipos de descoberta e fornece acesso aos perfis de entidades para investigar diferentes entidades envolvidas na descoberta. Uma entidade pode ser um Conta da AWS AWS recurso dentro de uma conta ou um endereço IP externo que tenha interagido com seus recursos. O console do GuardDuty oferece suporte à migração para o Amazon Detective a partir das seguintes entidades, dependendo do Conta da AWS tipo de descoberta: função do IAM, usuário ou sessão de função, agente do usuário, usuário federado, instância do Amazon EC2 ou endereço IP.

Sumário

Habilitar a integração

Para usar o Amazon Detective com o GuardDuty, você deve primeiro habilitar o Amazon Detective. Para obter informações sobre como habilitar o Detective, consulte Configurando o Amazon Detective no Guia de Administração do Amazon Detective.

Ao habilitar tanto o GuardDuty quanto o Detective, a integração é habilitada automaticamente. Depois de habilitado, o Detective consumirá imediatamente seus dados de descobertas do GuardDuty.

> **Note**
>
> O GuardDuty envia as descobertas ao Detective com base na frequência de exportação das descobertas do GuardDuty. Por padrão, a frequência de exportação para atualizações das descobertas existentes é de 6 horas. Para garantir que o Detective receba as atualizações mais recentes de suas descobertas, é recomendável alterar a frequência de exportação para 15 minutos em cada região em que você usa o Detective com o GuardDuty. Para mais informações, consulte Etapa 5 — Definindo a frequência para exportar descobertas ativas atualizadas.

Passando para o Amazon Detective a partir de uma descoberta do GuardDuty

1. Faça login no console em https://console.aws.amazon.com/guardduty.
2. Escolha uma única descoberta da sua tabela de descobertas.
3. Escolha Investigar com Detective no painel de detalhes da descoberta.
4. Escolha um aspecto da descoberta para investigar com o Amazon Detective. Isso abre o console do Detective para essa descoberta ou entidade.

Se o pivô não se comportar conforme o esperado, consulte Solução de problemas do pivô no Guia do usuário do Amazon Detective.

> **Note**
>
> Se você arquivar uma descoberta do GuardDuty no console do Detective, essa descoberta também será arquivada no console do GuardDuty.

Usando a integração com um ambiente de várias contas GuardDuty

Se você estiver gerenciando um ambiente de várias contas no GuardDuty, você deve adicionar suas contas-membro ao Amazon Detective para ver as visualizações de dados do Detective sobre descobertas e entidades nessas contas.

É recomendável usar a mesma conta de administrador do GuardDuty que a conta de administrador de Detective. Para obter mais informações sobre como adicionar contas-membro no Detective, consulte Convidar contas-membro.

> **Note**
>
> Detective é um serviço regional, o que significa que você deve habilitar o Detective e adicionar suas contas-membro em cada região na qual deseja usar a integração.

Suspendendo ou desativando GuardDuty

Você pode usar o GuardDuty console para suspender ou desativar o GuardDuty serviço. Você não é cobrado pelo uso GuardDuty quando o serviço é suspenso.

- Todas as contas dos membros devem ser desassociadas ou excluídas antes que você possa suspendê-las ou desativá-las. GuardDuty
- Se você suspender GuardDuty, ele não monitora mais a segurança do seu AWS ambiente nem gera novas descobertas. Suas descobertas existentes permanecem intactas e não são afetadas pela GuardDuty suspensão. Você pode optar por reativar GuardDuty mais tarde.
- Quando você desabilita GuardDuty em uma conta, ela será desativada somente para a atualmente selecionada Região da AWS. Se você quiser desativá-lo completamente GuardDuty, você deve desativá-lo em cada região em que ele está ativado.
- Se você desabilitar GuardDuty, suas descobertas e a GuardDuty configuração existentes serão perdidas e não poderão ser recuperadas. Se quiser salvar suas descobertas existentes, você deve exportá-las antes de confirmar a desativação GuardDuty. Para obter informações sobre como exportar descobertas, consulte Exportar descobertas.

Para suspender ou desativar GuardDuty

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, selecione Configurações.
3. Na GuardDuty seção Suspender, escolha Suspender GuardDuty ou Desativar e, em seguida GuardDuty, Confirme sua ação.

Para reativar GuardDuty após a suspensão

1. Abra o GuardDuty console em https://console.aws.amazon.com/guardduty/.
2. No painel de navegação, selecione Configurações.
3. Escolha Reativar GuardDuty.

Inscrever-se para receber anúncios do Amazon GuardDuty SNS

Esta seção fornece informações sobre a assinatura do Amazon SNS (Simple Notification Service) GuardDuty para receber anúncios sobre tipos de descoberta recém-lançados, atualizações dos tipos de descoberta existentes e outras alterações de funcionalidade. As notificações estão disponíveis em todos os formatos compatíveis com o Amazon SNS.

O GuardDuty SNS envia anúncios sobre atualizações do GuardDuty serviço AWS para qualquer conta assinada. Para receber notificações sobre descobertas em sua conta, consulte Criação de respostas personalizadas às GuardDuty descobertas com a Amazon CloudWatch Events.

> **Note**
>
> Seu usuário do IAM deve ter permissões `sns::subscribe` para a inscrição em um SNS.

Você pode se inscrever uma fila do Amazon SQS neste tópico de notificação, mas deve usar um ARN de tópico que esteja na mesma região. Para obter mais informações, consulte Tutorial: Inscrever-se em uma fila do Amazon SQS para um tópico do Amazon SNS no Guia do desenvolvedor do Amazon Simple Queue Service.

Você também pode usar uma AWS Lambda função para acionar eventos quando as notificações são recebidas. Para obter mais informações, consulte Invocar funções do Lambda usando notificações do Amazon SNS no Guia do desenvolvedor do Amazon Simple Queue Service.

Os ARNs do tópico do Amazon SNS de cada região são mostrados abaixo.

AWS Região	Tópico ARN do Amazon SNS
`us-east-1`	`arn:aws:sns:us-east-1:242987662583:GuardDutyAnnouncements`
`us-east-2`	`arn:aws:sns:us-east-2:118283430703:G`

AWS Região	Tópico ARN do Amazon SNS
	uardDutyAnnounceme nts
us-west-1	arn:aws:sns:us-wes t-1:144182107116:G uardDutyAnnounceme nts
us-west-2	arn:aws:sns:us-wes t-2:934957504740:G uardDutyAnnounceme nts
ca-central-1	arn:aws:sns:ca-cen tral-1:10743005193 3:GuardDutyAnnounc ements
ca-west-1	arn:aws:sns:ca-wes t-1:440427180217:G uardDutyAnnounceme nts
eu-north-1	arn:aws:sns:eu-nor th-1:973841112453: GuardDutyAnnouncem ents
eu-west-1	arn:aws:sns:eu-wes t-1:965013871422:G uardDutyAnnounceme nts

AWS Região	Tópico ARN do Amazon SNS
eu-west-2	arn:aws:sns:eu-west-2:506403581195:GuardDutyAnnouncements
eu-west-3	arn:aws:sns:eu-west-3:436163563069:GuardDutyAnnouncements
eu-central-1	arn:aws:sns:eu-central-1:378365507264:GuardDutyAnnouncements
eu-central-2	arn:aws:sns:eu-central-2:383009515534:GuardDutyAnnouncements
ap-east-1	arn:aws:sns:ap-east-1:646602203151:GuardDutyAnnouncements
ap-northeast-1	arn:aws:sns:ap-northeast-1:741172661024:GuardDutyAnnouncements
ap-northeast-2	arn:aws:sns:ap-northeast-2:464168911255:GuardDutyAnnouncements

AWS Região	Tópico ARN do Amazon SNS
ap-southeast-1	arn:aws:sns:ap-southeast-1:476419727788:GuardDutyAnnouncements
ap-southeast-2	arn:aws:sns:ap-southeast-2:457615622431:GuardDutyAnnouncements
ap-south-1	arn:aws:sns:ap-south-1:926826061926:GuardDutyAnnouncements
sa-east-1	arn:aws:sns:sa-east-1:955633302743:GuardDutyAnnouncements
us-gov-west-1	arn:aws-us-gov:sns:us-gov-west-1:430639793359:GuardDutyAnnouncements
cn-north-1	arn:aws-cn:sns:cn-north-1:002991280229:GuardDutyAnnouncements
cn-northwest-1	arn:aws-cn:sns:cn-northwest-1:003033775354:GuardDutyAnnouncements

AWS Região	Tópico ARN do Amazon SNS
me-south-1	arn:aws:sns:me-south-1:552740612889:GuardDutyAnnouncements
me-central-1	arn:aws:sns:me-central-1:030935290150:GuardDutyAnnouncements
eu-south-1	arn:aws:sns:eu-south-1:188461706213:GuardDutyAnnouncements
eu-south-2	arn:aws:sns:eu-south-2:445632894446:GuardDutyAnnouncements
us-gov-east-1	arn:aws:sns:us-gov-east-1:143972945659:GuardDutyAnnouncements
ap-northeast-3	arn:aws:sns:ap-northeast-3:129086577509:GuardDutyAnnouncements
ap-southeast-3	arn:aws:sns:ap-southeast-3:225965583551:GuardDutyAnnouncements

AWS Região	Tópico ARN do Amazon SNS
ap-south-2	arn:aws:sns:ap-south-2:595653072700:GuardDutyAnnouncements
ap-southeast-4	arn:aws:sns:ap-southeast-4:529900636122:GuardDutyAnnouncements
il-central-1	arn:aws:sns:il-central-1:847886274986:GuardDutyAnnouncements

Para assinar o e-mail de notificação de GuardDuty atualização no AWS Management Console

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Na lista de regiões, escolha a mesma região que o ARN do tópico que deseja assinar. Este exemplo usa a região `us-west-2`.
3. No painel de navegação à esquerda, escolha Subscriptions (Assinaturas), Create subscription (Criar assinatura).
4. Na caixa de diálogo Create Subscription (Criar assinatura), em Topic ARN (ARN do tópico), cole o ARN do tópico: `arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements`.
5. Em Protocolo, escolha Email. Em Endpoint, digite um endereço de e-mail que você pode usar para receber a notificação.
6. Selecione Criar assinatura.
7. Em seu aplicativo de e-mail, abra a mensagem em AWS Notificações e abra o link para confirmar sua assinatura.

   O navegador da Web exibe uma resposta de confirmação do Amazon SNS.

Para assinar o e-mail de notificação de GuardDuty atualização com o AWS CLI

1. Execute o seguinte comando com a AWS CLI:

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. Em seu aplicativo de e-mail, abra a mensagem em AWS Notificações e abra o link para confirmar sua assinatura.

   O navegador da Web exibe uma resposta de confirmação do Amazon SNS.

Formato da mensagem do Amazon SNS

Um exemplo de mensagem de notificação de GuardDuty atualização sobre novas descobertas é mostrado abaixo:

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FINDINGS\",\"findingDetails
\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"findingDescription\":\"This finding informs you that an EC2 instance in your AWS
 environment is making connections to a Tor Guard or an Authority node. Tor is software
 for enabling anonymous communication. Tor Guards and Authority nodes act as initial
 gateways into a Tor network. This traffic can indicate that this EC2 instance is
 acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised.\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
```

```
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

O valor da mensagem analisada (sem aspas com escape) é mostrado abaixo:

```
{
    "version": "1",
    "type": "NEW_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "findingDescription": "This finding informs you that an EC2 instance in your
 AWS environment is making connections to a Tor Guard or an Authority node. Tor is
 software for enabling anonymous communication. Tor Guards and Authority nodes act as
 initial gateways into a Tor network. This traffic can indicate that this EC2 instance
 is acting as a client on a Tor network. A common use for a Tor client is to circumvent
 network monitoring and filter for access to unauthorized or illicit content. Tor
 clients can also generate nefarious Internet traffic, including attacking SSH servers.
 This activity can indicate that your EC2 instance is compromised."
    }]
}
```

Um exemplo de mensagem de notificação de GuardDuty atualização sobre atualizações de GuardDuty funcionalidade é mostrado abaixo:

```
{
    "Type" : "Notification",
    "MessageId" : "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn" : "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message" : "{\"version\":\"1\",\"type\":\"NEW_FEATURES\",\"featureDetails
\":[{\"featureDescription\":\"Customers with high-volumes of global CloudTrail
 events should see a net positive impact on their GuardDuty costs.\",\"featureLink
\":\"https://docs.aws.amazon.com//guardduty/latest/ug/guardduty_data-
sources.html#guardduty_cloudtrail\"}]}",
    "Timestamp" : "2018-03-09T00:25:43.483Z",
    "SignatureVersion" : "1",
    "Signature" : "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
```

```
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
    "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

O valor da mensagem analisada (sem aspas com escape) é mostrado abaixo:

```
{
    "version": "1",
    "type": "NEW_FEATURES",
    "featureDetails": [{
        "featureDescription": "Customers with high-volumes of global CloudTrail events
 should see a net positive impact on their GuardDuty costs.",
        "featureLink": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_data-sources.html#guardduty_cloudtrail"
    }]
}
```

Um exemplo de mensagem de notificação de GuardDuty atualização sobre descobertas atualizadas é mostrado abaixo:

```
{
    "Type": "Notification",
    "MessageId": "9101dc6b-726f-4df0-8646-ec2f94e674bc",
    "TopicArn": "arn:aws:sns:us-west-2:934957504740:GuardDutyAnnouncements",
    "Message": "{\"version\":\"1\",\"type\":\"UPDATED_FINDINGS\",
\"findingDetails\":[{\"link\":\"https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html\",\"findingType\":\"UnauthorizedAccess:EC2/TorClient\",
\"description\":\"Increased severity value from 5 to 8.\"}]}",
    "Timestamp": "2018-03-09T00:25:43.483Z",
    "SignatureVersion": "1",
    "Signature": "XWox8GDGLRiCgDOXlo/
fG9Lu/88P8S0FL6M6oQYOmUFzkucuhoblsdea3BjqdCHcWR7qdhMPQnLpN7y9iBrWVUqdAGJrukAI8athvAS
+4AQD/V/QjrhsEnlj+GaiW
+ozAu006X6GopOzFGnCtPMROjCMrMonjz7Hpv/8KRuMZR3pyQYm5d4wWB7xBPYhUMuLoZ1V8YFs55FMtgQV/
YLhSYuEu0BP1GMtLQauxDkscOtPP/vjhGQLFx1Q9LTadcQiRHtNIBxWL87PSI
+BVvkin6AL7PhksvdQ7FAgHfXsit+6p8GyOvKCqaeBG7HZhR1AbpyVka7JSNRO/6ssyrlj1g==",
```

```
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-433026a4050d206028891664da859041.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:934957504740:GuardDutyAnnouncements:9225ed2b-7228-4665-8a01-c8a5db6859f4"
}
```

O valor da mensagem analisada (sem aspas com escape) é mostrado abaixo:

```
{
    "version": "1",
    "type": "UPDATED_FINDINGS",
    "findingDetails": [{
        "link": "https://docs.aws.amazon.com//guardduty/latest/ug/
guardduty_unauthorized.html",
        "findingType": "UnauthorizedAccess:EC2/TorClient",
        "description": "Increased severity value from 5 to 8."
    }]
}
```

Cotas para a Amazon GuardDuty

Sua conta da AWS possui cotas padrão, anteriormente chamadas de limites, para cada produto da AWS. A menos que especificado de outra forma, cada cota é específica da região . Você pode solicitar o aumento de algumas cotas, porém, algumas delas não podem ser aumentadas.

Para ver as cotas GuardDuty, abra o console Service Quotas. No painel de navegação, escolha AWSserviços e selecione Amazon GuardDuty.

Para solicitar um aumento da cota, consulte Requesting a quota increase no Guia do usuário do Service Quotas.

Sua AWS conta tem as seguintes cotas para a Amazon GuardDuty por região.

> **Note**
>
> Para cotas específicas para proteção contra GuardDuty malware, consulteCotas de Proteção contra malware.

Recurso	Padrão	Comentários
Detectores	1	O número máximo de recursos do detector que você pode criar por conta da AWS por região. Não é possível solicitar um aumento da cota.
Filtros	100	O número máximo de filtros salvos por conta da AWS por região.

Recurso	Padrão	Comentários
		Não é possível solicitar um aumento da cota.
Período de retenção da descoberta	90 dias	O número máximo de dias em que uma descoberta é mantida. Não é possível solicitar um aumento da cota.
Endereços IP e intervalos de CIDR por lista de IPs confiáveis	2.000	O número máximo de endereços IP e intervalos de CIDR que você pode incluir em uma única lista de IPs confiáveis. Não é possível solicitar um aumento da cota.
Endereços IP e intervalos de CIDR por lista de ameaças	250.000	O número máximo de endereços IP e intervalos de CIDR que você pode incluir em uma lista de ameaças. Não é possível solicitar um aumento da cota.

Recurso	Padrão	Comentários
Tamanho máximo do arquivo	35 MB	O tamanho máximo de arquivo usado para fazer upload de uma lista de endereços IP ou intervalos de CIDR a serem incluídos em uma lista de IPs confiáveis ou em uma lista de ameaças. Não é possível solicitar um aumento da cota.
Contas-membro (por convite)	5000	O número máximo de contas de membros associadas a uma conta de administrador.
Contas-membro	50.000	O número máximo de contas de membros associadas a uma conta de administrador por meio deAWS Organizations. Isso inclui contas-membro que são adicionadas à organização por convite.

Recurso	Padrão	Comentários
Conjuntos de inteligência de ameaças	6	O número máximo de conjuntos de inteligência de ameaças que você pode adicionar por conta da AWS por região. Não é possível solicitar um aumento da cota.
Conjuntos de IPs confiáveis	1	O número máximo de conjuntos de IPs confiáveis que podem ser carregados e habilitados por conta da AWS por região. Não é possível solicitar um aumento da cota.

Solução de problemas da Amazon GuardDuty

Quando você receber problemas relacionados à execução de uma ação específica GuardDuty, consulte os tópicos desta seção.

Tópicos

Problemas gerais em GuardDuty

Estou recebendo um erro de acesso ao exportar GuardDuty as descobertas. Como posso resolver isso?

Depois de definir as configurações para exportar descobertas, se não GuardDuty for possível exportar descobertas, ele exibirá uma mensagem de erro na página Configurações no GuardDuty console. Isso pode acontecer quando GuardDuty você não consegue mais acessar o recurso de destino, por exemplo, se seu bucket do Amazon S3 foi excluído ou a permissão para acessar o bucket foi modificada. Isso também pode acontecer quando GuardDuty você não consegue mais acessar a AWS KMS chave que foi usada para criptografar os dados em seu bucket do Amazon S3. Quando GuardDuty não consegue exportar, ele envia uma notificação para o e-mail associado à conta para fornecer informações sobre esse problema.

Para resolver o problema, certifique-se de que os recursos correspondentes existam e GuardDuty tenham as permissões para acessar os recursos necessários. Se você não resolver o problema antes que o período de retenção de descobertas de 90 dias termine GuardDuty, suas descobertas não serão exportadas. GuardDuty desativará a localização de configurações de exportação para essa conta na região específica. Mesmo após essa data de retenção, você pode atualizar as configurações para reiniciar a exportação das descobertas na região específica.

Para ter mais informações, consulte Exportar descobertas.

Problemas de proteção contra malware

Estou iniciando uma verificação de malware sob demanda, mas isso resulta na falta de um erro de permissões necessárias.

Se você receber um erro sugerindo que você não tem as permissões necessárias para iniciar uma verificação de malware sob demanda em uma instância do Amazon EC2, verifique se você anexou a política AWS política gerenciada: AmazonGuardDutyFullAccess ao seu perfil do IAM.

Se você for membro de uma AWS organização e ainda receber o mesmo erro, conecte-se à sua conta de gerenciamento. Para ter mais informações, consulte AWS Organizations SCP — Acesso negado.

Eu recebo uma mensagem de erro do **`iam:GetRole`** ao trabalhar com a Proteção contra malware.

Se você receber esse erro —`Unable to get role: AWSServiceRoleForAmazonGuardDutyMalwareProtection`, significa que você está perdendo a permissão para ativar a verificação de malware GuardDuty iniciada ou usar a verificação de malware sob demanda. Verifique se você anexou a política AWS política gerenciada: AmazonGuardDutyFullAccess ao seu perfil do IAM.

Sou uma conta de GuardDuty administrador que precisa ativar a verificação de GuardDuty malware iniciada, mas não usa a política AWS gerenciada: AmazonGuardDutyFullAccess para gerenciar GuardDuty.

- Configure a função do IAM que você usa GuardDuty para ter as permissões necessárias para ativar a verificação GuardDuty de malware iniciada. Para obter mais informações sobre as permissões necessárias, consulte Criação de uma função vinculada ao serviço para Proteção contra malware.
- Anexar a AWS política gerenciada: AmazonGuardDutyFullAccess ao seu perfil do IAM. Isso ajudará você a ativar a verificação GuardDuty de malware iniciada nas contas dos membros.

Problemas de monitoramento de tempo de execução

Meu AWS Step Functions fluxo de trabalho está falhando inesperadamente

Se o GuardDuty contêiner contribuiu para a falha do fluxo de trabalho, consulteSolução de problemas de cobertura. Se o problema persistir, para evitar a falha do fluxo de trabalho devido ao GuardDuty contêiner, execute uma das seguintes etapas:

- Adicione a `false` tag`GuardDutyManaged`: ao cluster Amazon ECS associado.
- Desative a configuração automática do agente para AWS Fargate (somente ECS) no nível da conta. Adicione a tag de inclusão`GuardDutyManaged`: `true` ao cluster Amazon ECS associado que você deseja continuar monitorando com o agente GuardDuty automatizado.

Solução de problemas de falta de memória no Runtime Monitoring (somente suporte ao Amazon EC2)

Esta seção fornece as etapas de solução de problemas quando você enfrenta um erro de falta de memória com base na Limite de CPU e memória implantação manual do agente de GuardDuty segurança.

Se `systemd` encerrar o GuardDuty agente por causa do `out-of-memory` problema e você avaliar que fornecer mais memória ao GuardDuty agente é razoável, você pode atualizar o limite.

1. Com a permissão do root, abra`/lib/systemd/system/amazon-guardduty-agent.service`.
2. Encontre `MemoryLimit` e `MemoryMax` e atualize os dois valores.

```
MemoryLimit=256MB
MemoryMax=256MB
```

3. Depois de atualizar os valores, reinicie o GuardDuty agente usando o seguinte comando:

```
sudo systemctl daemon-reload
sudo systemctl restart amazon-guardduty-agent
```

4. Execute o comando a seguir para ver o status:

```
sudo systemctl status amazon-guardduty-agent
```

A saída esperada mostrará o novo limite de memória:

```
Main PID: 2540 (amazon-guardduty)
Tasks: 16
Memory: 21.9M (limit: 256.0M)
```

Gerenciamento de problemas com várias contas

Quero gerenciar várias contas, mas não tenho a permissão AWS Organizations de gerenciamento necessária.

Se você receber esse erro —`The request failed because you do not have required AWS Organization master permission.`, isso significa que você está perdendo a permissão para ativar a verificação de GuardDuty malware iniciada para várias contas em sua organização. Para obter mais informações sobre como fornecer permissão para a conta de gerenciamento, consulteEstabelecendo acesso confiável para permitir a GuardDuty verificação de malware iniciada.

Outros problemas de solução de problemas

Se você não encontrar um cenário adequado ao seu problema, veja as seguintes opções de solução de problemas:

- Para problemas gerais do IAM ao acessar o https://console.aws.amazon.com/guardduty/, consulte Solução de problemas de GuardDuty identidade e acesso da Amazon.
- Para problemas de autenticação e autorização durante o acesso AWS AWS Console Home, consulte Solução de problemas do IAM.

Regiões e endpoints

Para ver Regiões da AWS onde a Amazon GuardDuty está disponível, consulte os GuardDuty endpoints da Amazon no Referência geral da Amazon Web Services.

Recomendamos que você ative GuardDuty em todos os compatíveis Regiões da AWS. Isso permite GuardDuty gerar descobertas sobre atividades não autorizadas ou incomuns, mesmo em regiões que você não está usando ativamente. Isso também permite GuardDuty monitorar AWS CloudTrail eventos para o suportado Regiões da AWS, reduzindo sua capacidade de detectar atividades que envolvam serviços globais.

Disponibilidade de recursos específicos da região

Uma lista de diferenças regionais para especificar a disponibilidade dos GuardDuty recursos.

ListFindings e GetFindingsStatistics APIs

As ListFindingsAPIs GetFindingsStatisticse têm um `consoleOnly` sinalizador temporário. Quando você usa qualquer uma dessas APIs ou ambas, a `consoleOnly` sinalização significa que a API pode buscar resultados até um limite máximo de 1000.

GuardDuty características com disparidade regional

GuardDuty Proteção contra malware

GuardDuty suporta o recurso de Proteção contra Malware nas Zonas Locais AWS Dedicadas.

GuardDuty Monitoramento de execução

Atualmente, o recurso Runtime Monitoring não é suportado na região Oeste do Canadá (Calgary).

GuardDuty Proteção RDS

A lista a seguir especifica Regiões da AWS onde a Proteção RDS atualmente não é suportada:

- Oeste do Canadá (Calgary)
- Ásia-Pacífico (Hyderabad)
- Europa (Espanha)
- Europa (Zurique)

- Oriente Médio (Emirados Árabes Unidos)
- Israel (Tel Aviv)
- Ásia-Pacífico (Melbourne)

As seguintes APIs na Amazon GuardDuty API Reference podem ter diferenças regionais devido à indisponibilidade de algumas das fontes de dados ou recursos especificados anteriormente: Regiões da AWS

- CreateDetector
- UpdateDetector
- UpdateMemberDetectors
- UpdateOrganizationConfiguration
- GetDetector
- GetMemberDetectors
- DescribeOrganizationConfiguration

Tipos de descoberta do Amazon EC2: DefenseEvasion:EC2/UnusualDoHActivity e DefenseEvasion:EC2/UnusualDoTActivity

A tabela a seguir mostra Regiões da AWS onde GuardDuty está disponível, mas esses dois tipos de descoberta do Amazon EC2 ainda não são suportados.

Região da AWS	Código da região
Ásia-Pacífico (Seul)	ap-northeast-2
Asia Pacific (Osaka)	ap-northeast-3
Ásia-Pacífico (Jacarta)	ap-southeast-3

AWS GovCloud (US) Regiões

Para obter as informações mais recentes, consulte Amazon GuardDuty no Guia AWS GovCloud (US) do usuário.

Regiões da China

Para obter as informações mais recentes, consulte Disponibilidade de atributos e diferenças de implementação.

GuardDuty ações e parâmetros legados

GuardDuty A Amazon descontinuou algumas das ações e parâmetros da API, mas ainda os suporta. A prática recomendada é usar as novas ações e parâmetros da API que substituem as opções legadas. A tabela a seguir compara as ações e os parâmetros antigos e novos.

Ações/parâmetros legados	Novas ações/parâmetros	Comparação
DisassociateFromMasterAccount	DisassociateFromAdministratorAccount	Com a mesma implementação em ambas as ações, GuardDuty usa o termo `Administrator` em`DisassociateFromAdministratorAccount` .
`autoEnable` parâmetro em DescribeOrganizationConfiguratione UpdateOrganizationConfiguration	`autoEnableOrganizationMembers`	Com`autoEnableOrganizationMembers` , a conta GuardDuty do administrador pode auditar e aplicar GuardDuty qualquer um dos valores em todas as contas dos membros. Usando as APIs, pode levar até 24 horas para atualizar a configuração de todas as contas-membro. Para obter mais informações sobre os valores possíveis do `autoEnableOrganizationMembers` campo, consulte autoEnableOrganizationMembros
Parâmetro `dataSources` nas APIs listadas em GuardDuty Mudanças na API em março de 2023.	`features`	A partir de março de 2023, você pode configurar Proteção contra malware na Amazon GuardDuty e usar os novos planos de GuardDuty proteção`features`. Os planos de proteção lançados antes de março de 2023, incluindo a Proteção contra malware, ainda oferecem

Ações/parâmetros legados	Novas ações/parâmetros	Comparação
		suporte à configuração que usa `dataSources` . Se você usa APIs para configurar um plano de proteção, cada solicitação de API pode incluir `dataSources` ou `features`, mas não ambos.

Histórico de documentos da Amazon GuardDuty

A tabela a seguir descreve mudanças importantes na documentação desde a última versão do Guia do GuardDuty usuário da Amazon. Para receber notificações sobre atualizações dessa documentação, você poderá se inscrever em um feed RSS.

Alteração	Descrição	Data
Experiência de console atualizada para configurar as descobertas de exportação	GuardDuty atualizou a experiência do console para exportar as descobertas geradas em seu Contas da AWS, para um bucket do Amazon S3. Para obter mais informações, consulte Exportação de GuardDuty descobertas.	1 de abril de 2024
Funcionalidade atualizada no Runtime Monitoring	O Runtime Monitoring lançou um novo agente de segurança versão 1.1.0 para o recurso Amazon EC2. Esta versão oferece suporte à configura ção GuardDuty automatiz ada de agentes no Runtime Monitoring para instâncias do Amazon EC2. Para obter informações sobre as notas de lançamento, consulte o agente GuardDuty de segurança para a instância do Amazon EC2.	28 de março de 2024
Disponibilidade geral do Runtime Monitoring para instâncias do Amazon EC2	GuardDuty anuncia a disponibi lidade geral (GA) do Runtime Monitoring para instância s do Amazon EC2. Agora, você tem a opção de ativar	28 de março de 2024

a configuração automática do agente que permite GuardDuty instalar e gerenciar o agente de segurança para suas instâncias do Amazon EC2 em seu nome. Com o agente GuardDuty automatizado, você também pode usar tags de inclusão ou exclusão GuardDuty para informar a instalação e o gerenciamento do agente de segurança somente em instâncias selecionadas do Amazon EC2. Para obter mais informações, consulte Como o Runtime Monitoring funciona com instâncias do Amazon EC2.

Lista de novos tipos de descobertas lançados junto com este GA

- Execução: Tempo de execução/ SuspiciousTool
- Execução: Tempo de execução/ SuspiciousCommand
- DefenseEvasion:Tempo de execução/ SuspiciousCommand
- DefenseEvasion:Tempo de execução/ PtraceAntiDebugging

- Execução: Tempo de execução/ MaliciousFileExecuted

A Amazon GuardDuty atualizou a função vinculada ao serviço (SLR)	Use AWS Systems Manager ações para gerenciar associações de SSM em instâncias do Amazon EC2 ao GuardDuty ativar o Runtime Monitoring com um agente automatizado para o Amazon EC2. Quando a configuração GuardDuty automatizada do agente está desativada, GuardDuty considera somente as instâncias do EC2 que têm uma tag de inclusão (`GuardDuty Managed :true`). • A lista a seguir mostra as novas permissões: `"ssm:DescribeAssociation", "ssm:DeleteAssociation", "ssm:UpdateAssociation", "ssm:CreateAssociation", "ssm:StartAssociationsOnce", "ssm:AddTagsToResource", "ssm:CreateAssociation", "ssm:UpdateAssociation", "ssm:SendCommand", "ssm:GetCommandInvocation"`	26 de março de 2024

Funcionalidade atualizada no Runtime Monitoring	Com a versão mais recente do agente de GuardDuty segurança (complemento) v1.5.0 para o Amazon EKS, o Runtime Monitoring agora oferece suporte à configura ção de parâmetros específicos do seu agente de GuardDuty segurança, como configura ções de CPU e memória, `PriorityClass` configura ções e configurações de política de DNS. Para obter mais informações, consulte Configuração dos parâmetro s do agente GuardDuty de segurança (complemento EKS).	7 de março de 2024
Funcionalidade atualizada no Runtime Monitoring	O Runtime Monitoring lançou uma nova versão 1.5.0 do agente para recursos do Amazon EKS. Para obter informações sobre as notas de versão, consulte o histórico de lançamentos do agente complementar EKS.	7 de março de 2024

Support for Canada West (Calgary)	A Amazon agora GuardDuty está disponível na região Oeste do Canadá (Calgary) . Alguns dos planos de proteção incluídos GuardDuty podem não estar disponíveis nesta região. Para obter as informações mais recentes, consulte Regiões e endpoints.	6 de março de 2024
Funcionalidade atualizada no Runtime Monitoring	As versões 1.0.0 e 1.1.0 do agente de GuardDuty segurança para clusters Amazon EKS não serão mais suportadas a partir de 14 de maio de 2024. Para obter informações sobre quais etapas você pode tomar antes do final do suporte padrão, consulte o agente GuardDuty de segurança para clusters do Amazon EKS.	16 de fevereiro de 2024

Funcionalidade atualizada no Runtime Monitoring	O Runtime Monitoring é compatível com a versão 1.29 mais recente do Kubernetes com a versão 1.4.1 do agente de segurança existente. O suporte está disponível desde o lançamento desta versão do Kubernetes. Para obter informações sobre as versões compatíveis do Kubernetes, consulte Versões do Kubernetes suportadas pelo agente de segurança. GuardDuty	16 de fevereiro de 2024

Funcionalidade atualizada no Runtime Monitoring - Disponibilidade regional	GuardDuty O Runtime Monitoring agora oferece suporte ao Amazon VPC compartilhado dentro do mesmo. AWS Organizations GuardDuty a função vinculada ao serviço (SLR) tem uma nova permissão, `organizations:DescribeOrganization` que ajuda a recuperar o ID da organização da conta compartilhada da Amazon VPC para definir a política de endpoint. Para obter informações sobre os pré-requisitos para usar um endpoint compartilhado da Amazon VPC no Runtime Monitoring, consulte Support for shared Amazon VPC. Esse recurso está disponível em todas as regiões que oferecem GuardDuty suporte ao monitoramento de tempo de execução.	12 de fevereiro de 2024

Funcionalidade atualizada no Runtime Monitoring - Disponibilidade regional	GuardDuty O Runtime Monitoring agora oferece suporte ao Amazon VPC compartilhado dentro do mesmo. AWS Organizations GuardDuty a função vinculada ao serviço (SLR) tem uma nova permissão, `organizations:DescribeOrganization` que ajuda a recuperar o ID da organização da conta compartilhada da Amazon VPC para definir a política de endpoint. Para obter informações sobre os pré-requisitos para usar um endpoint compartilhado da Amazon VPC no Runtime Monitoring, consulte Support for shared Amazon VPC. Atualmente, esse recurso está disponível em alguns dos Regiões da AWS. Para obter mais informações, consulte Regiões e endpoints da .	9 de fevereiro de 2024
Funcionalidade atualizada com suporte para o novo Regiões da AWS — Proteção contra malware	A Proteção contra Malware agora suporta a verificação dos volumes do EBS criptografados Chaves gerenciadas pela AWS na região Oeste dos EUA (Oregon).	6 de fevereiro de 2024

Funcionalidade atualizada com suporte para o novo Regiões da AWS — Proteção contra malware	O Malware Protection agora suporta a verificação dos volumes do EBS Chaves gerenciadas pela AWS criptografados com o seguinte: Regiões da AWS • Ásia-Pacífico (Singapura) (`ap-southeast-1`) • Europa (Frankfurt) (`eu-central-1`) • Asia Pacific (Osaka) (`ap-northeast-3`) • Leste dos EUA (Ohio) (`us-east-2`) • Europa (Milão) (`eu-south-1`) • Ásia-Pacífico (Tóquio) (`ap-northeast-1`) • Ásia-Pacífico (Seul) (`ap-northeast-2`) • Canadá (Central) (`ca-central-1`) • Europa (Irlanda) (`eu-west-1`) • Leste dos EUA (Norte da Virgínia) (`us-east-1`)	5 de fevereiro de 2024

Funcionalidade atualizada no Runtime Monitoring	GuardDuty O Runtime Monitoring lançou uma nova versão do agente de GuardDuty segurança (v1.0.2) para instâncias do Amazon EC2. Essa versão do agente inclui suporte para as AMIs mais recentes do Amazon ECS. Para obter mais informações sobre o histórico de lançamentos de agentes, consulte Agente GuardDuty de segurança para instâncias do Amazon EC2.	2 de fevereiro de 2022

Funcionalidade atualizada com suporte para o novo Regiões da AWS — Proteção contra malware	O Malware Protection agora suporta a verificação dos volumes do Amazon EBS Chaves gerenciadas pela AWS criptografados com o seguinte: Regiões da AWS • Europa (Londres) (`eu-west-2`) • Europa (Estocolmo) (`eu-north-1`) • Ásia-Pacífico (Hong Kong) (`ap-east-1`) • África (Cidade do Cabo) (`af-south-1`) • Oriente Médio (Bahrein) (`me-south-1`) • Asia Pacific (Hyderabad) (`ap-south-2`) • Europa (Espanha) (`eu-south-2`) • Ásia-Pacífico (Melbourne) (`ap-southeast-4`) • Ásia-Pacífico (Sydney) (`ap-southeast-2`) • Israel (Tel Aviv) (`il-central-1`)	31 de janeiro de 2024

Gerenciamento de contas atualizado com AWS Organizations	Reorganizou o conteúdo em Gerenciando contas com AWS Organizations. , adicionou etapas para alterar a conta do GuardDuty administrador delegado e atualizou Compreendendo a relação entre a conta do GuardDuty administrador e as contas dos membros.	30 de janeiro de 2024
Funcionalidade atualizada com suporte para novos Regiões da AWS	O Malware Protection agora suporta a verificação dos volumes do EBS Chaves gerenciadas pela AWS criptografados com o seguinte: Regiões da AWS • Ásia-Pacífico (Jacarta) (`ap-southeast-3`) • Oeste dos EUA (N. da Califórnia) (`us-west-1`) • Oriente Médio (Emirados Árabes Unidos) (`me-central-1`) • Europa (Zurique) (`eu-central-2`) • Ásia-Pacífico (Mumbai) (`ap-south-1`) • América do Sul (São Paulo) (`sa-east-1`)	29 de janeiro de 2024

Funcionalidade atualizada na proteção contra malware	A Proteção contra Malware agora suporta a verificação dos volumes do EBS criptografados usando Chaves gerenciadas pela AWS. A função vinculada ao serviço (SLR) de proteção contra malware tem duas novas permissões — e. `GetSnapshotBlock` `ListSnapshotBlocks` Essas permissões ajudarão a GuardDuty obter o instantâneo de um volume do EBS (usando criptografia Chave gerenciada pela AWS) do seu Conta da AWS e copiá-lo para a conta de GuardDuty serviço antes de iniciar a verificação de malware. Atualmente, essa funcionalidade está disponível somente na Europa (Paris) (`eu-west-3`). Para obter mais informações, consulte Volumes suportados para verificação de malware.	25 de janeiro de 2024

Funcionalidade atualizada no Runtime Monitoring	GuardDuty O Runtime Monitoring lançou uma nova versão do agente de GuardDuty segurança (v1.0.1) com ajustes e aprimoramentos gerais de desempenho. Para obter mais informações sobre o histórico de lançamentos de agentes, consulte Agente GuardDuty de segurança para instâncias do Amazon EC2.	23 de janeiro de 2024
Funcionalidade atualizada no Runtime Monitoring	O Runtime Monitoring lançou uma nova versão 1.4.1 do agente para recursos do Amazon EKS. Para obter mais informações, consulte o Histórico de versões do agente complementar do EKS.	16 de janeiro de 2024
O Runtime Monitoring lançou um novo agente v1.4.0 para recursos do Amazon EKS	O Runtime Monitoring lançou uma nova versão 1.4.0 do agente para os recursos do Amazon EKS. Para obter mais informações, consulte o Histórico de versões do agente complementar do EKS.	21 de dezembro de 2023

Foram adicionados tipos de descobertas baseadas em S3 e aprendizado de AWS CloudTrail máquina (ML) à Europa (Zurique), Europa (Espanha), Ásia-Pacífico (Hyderabad), Ásia-Pacífico (Melbourne) e Israel (Tel Aviv)	O seguinte S3 e as CloudTrail descobertas que identificam o comportamento anômalo usando o modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias estão agora disponíveis nas regiões da Europa (Zurique), Europa (Espanha), Ásia-Pacífico (Hyderabad), Ásia-Pacífico (Melbourne) e Israel (Tel Aviv): • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior	21 de dezembro de 2023

	• Persistence:IAMUser/AnomalousBehavior • PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	
GuardDuty suporta 50.000 contas de membros por meio de AWS Organizations	Agora, um GuardDuty administrador delegado pode gerenciar no máximo 50.000 contas de membros por meio do. AWS Organizations Isso também inclui um máximo de 5000 contas de membros associadas à conta de GuardDuty administrador por convite.	20 de dezembro de 2023

GuardDuty Suporte de monitoramento de tempo de execução expandido para 19 Regiões da AWS	O monitoramento de tempo de execução agora está disponível na Ásia-Pacífico (Jacarta), Europa (Paris), Ásia-Pacífico (Osaka), Ásia-Pacífico (Seul), Oriente Médio (Bahrein), Europa (Espanha), Ásia-Pacífico (Hyderabad), Ásia-Pacífico (Melbourne), Israel (Tel Aviv), Oeste dos EUA (Norte da Califórnia), Europa (Londres) , Ásia-Pacífico (Hong Kong), Europa (Milão), Oriente Médio (Emirados Árabes Unidos), América do Sul (São Paulo), Ásia-Pacífico (Mumbai), Canadá (Central), África (Cidade do Cabo), Europa (Zurique).	6 de dezembro de 2023
GuardDuty expande a capacidade de monitoramento de tempo de execução	Além de detectar ameaças aos seus clusters do Amazon EKS, GuardDuty anuncia a disponibilidade geral do Runtime Monitoring para detectar ameaças às suas cargas de trabalho do Amazon ECS e uma versão prévia para detectar ameaças às suas instâncias do Amazon EC2. Para obter mais informações sobre quais Regiões da AWS atualmente oferecem suporte ao Runtime Monitoring, consulte Regiões e endpoints.	26 de novembro de 2023

A Amazon GuardDuty atualizou a função vinculada ao serviço (SLR)	GuardDuty adicionou novas permissões para usar as ações do Amazon ECS para gerenciar e recuperar informações sobre os clusters do Amazon ECS e gerenciar a configuração da conta do Amazon ECS com. `guarddutyActivate` As ações relacionadas ao Amazon ECS também recuperam as informações sobre as tags associadas a. GuardDuty • As seguintes permissões foram adicionadas como parte da GuardDuty expansão do recurso de monitoramento de tempo de execução: `"ecs:ListClusters", "ecs:DescribeClusters", "ecs:PutAccountSettingDefault"`	26 de novembro de 2023
Atualizou as políticas AWS gerenciadas	GuardDuty adicionou uma nova permissão, `organizations:ListAccounts` ao AmazonGuardDutyFullAccessPolicyAmazonGuardDutyReadOnlyAccesse.	16 de novembro de 2023

GuardDuty lançou novos tipos de descoberta que usam o EKS Audit Log Monitoring.	O EKS Audit Log Monitoring agora suporta os seguintes tipos de descoberta na Ásia-Pacífico (Melbourne) (`ap-southeast-4`). • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	11 de novembro de 2023

GuardDuty lançou novos tipos de descoberta que usam o EKS Audit Log Monitoring.	O EKS Audit Log Monitoring agora suporta os seguintes tipos de descoberta nas regiões Ásia-Pacífico (Hyderabad`ap-south-2`) (), Europa (Zurique) (`eu-central-2`) e Europa (Espanha) (). `eu-south-2` • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated	10 de novembro de 2023

- Discovery:Kubernetes/AnomalousBehavior.PermissionChecked

GuardDuty lançou novos tipos de descoberta que usam o EKS Audit Log Monitoring.	O EKS Audit Log Monitoring agora suporta os seguintes tipos de descoberta. Esses tipos de descoberta ainda não estão disponíveis nas regiões Ásia-Pacífico (Hyderabad) (`ap-south-2`), Europa (Zurique) (`eu-central-2`), Europa (Espanha) (`eu-south-2`) e Ásia-Pacífico (Melbourne) (). `ap-southeast-4` • CredentialAccess:Kubernetes/AnomalousBehavior.SecretsAccessed • PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleBindingCreated • Execution:Kubernetes/AnomalousBehavior.ExecInPod • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!PrivilegedContainer • PrivilegeEscalation:Kubernetes/AnomalousBehavior.WorkloadDeployed!ContainerWithSensitiveMount • Execution:Kubernetes/AnomalousBehavior.WorkloadDeployed	8 de novembro de 2023

	• PrivilegeEscalation:Kubernetes/AnomalousBehavior.RoleCreated • Discovery:Kubernetes/AnomalousBehavior.PermissionChecked	
O Monitoramento de runtime do EKS lançou o novo agente v1.3.1	O EKS Runtime Monitoring lançou uma nova versão 1.3.1 do agente que inclui patches e atualizações de segurança importantes.	23 de outubro de 2023
Novo atributo de filtro para descoberta	GuardDuty adicionou um novo critério para filtrar as descobertas geradas. O sufixo do domínio de solicitação de DNS fornece o domínio de segundo e primeiro nível envolvido na atividade que solicitou GuardDuty a geração da descoberta.	17 de outubro de 2023
O Monitoramento de runtime do EKS lançou o novo agente v1.3.0 compatível com a versão 1.28 do Kubernetes	O EKS Runtime Monitoring lançou uma nova versão 1.3.0 do agente compatível com a versão 1.28 do Kubernetes. Foi adicionado suporte para Ubuntu. Para obter mais informações, consulte o Histórico de versões do agente complementar do EKS.	5 de outubro de 2023

Foram adicionados tipos de descobertas baseadas em S3 e aprendizado de AWS CloudTrail máquina (ML) às regiões Ásia-Pacífico (Jacarta) e Oriente Médio (EAU)	O seguinte S3 e as CloudTrail descobertas que identificam o comportamento anômalo usando o modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias estão agora disponíveis nas regiões Ásia-Pacífico (Jacarta) e Oriente Médio (EAU): • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior • Exfiltration:IAMUser/AnomalousBehavior • Impact:IAMUser/AnomalousBehavior • CredentialAccess:IAMUser/AnomalousBehavior • DefenseEvasion:IAMUser/AnomalousBehavior • InitialAccess:IAMUser/AnomalousBehavior • Persistence:IAMUser/AnomalousBehavior	20 de setembro de 2023

	• PrivilegeEscalation:IAMUser/AnomalousBehavior • Discovery:IAMUser/AnomalousBehavior	
GuardDuty O EKS Runtime Monitoring apresenta o gerenciamento GuardDuty de agentes de segurança no nível do cluster	O EKS Runtime Monitoring adiciona suporte para gerenciar o agente de GuardDuty segurança para clusters EKS individuais para monitorar os eventos de tempo de execução somente desses clusters seletivos. O Monitoramento de runtime do EKS amplia esse recurso com o suporte de tags.	13 de setembro de 2023
GuardDuty A proteção contra malware estende o suporte a mais Regiões da AWS	A Proteção contra malware está disponível na Ásia-Pacífico (Hyderabad), Ásia-Pacífico (Melbourne), Europa (Zurique) e Europa (Espanha).	11 de setembro de 2023

GuardDuty agora está disponível na região de Israel (Tel Aviv)	Foi adicionada a região de Israel (Tel Aviv) à lista de Regiões da AWS onde agora GuardDuty está disponível. Os seguintes planos de proteção também estão disponíveis na região Israel (Tel Aviv): • O GuardDuty Proteção EKS inclui Monitoramento de logs de auditoria do EKS e Monitoramento de runtime do EKS. • GuardDuty Proteção Lambda. • GuardDuty Proteção contra malware. • GuardDuty Proteção S3. Para obter mais informaçõ es sobre a disponibilidade do plano de proteção na região Israel (Tel Aviv), consulte Regiões e endpoints.	24 de agosto de 2023
GuardDuty adicionou configuração de ativação automática para sua organizaç ão no nível do plano de proteção	Atualize a configuração da organização para os planos de proteção em sua região. As opções de configuração possíveis são habilitar para todas as contas, habilitar automaticamente para novas contas ou não habilitar automaticamente para nenhuma conta em sua organização.	16 de agosto de 2023

Os tipos de descoberta do S3 que identificam comportamentos anômalos usando o modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias agora estão disponíveis na Ásia-Pacífico (Osaka)	Os seguintes tipos de descoberta estão disponíveis na região Ásia-Pacífico (Osaka): • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	10 de agosto de 2023
O Monitoramento de runtime do EKS está disponível na Ásia-Pacífico (Melbourne)	O EKS Runtime Monitoring dentro do GuardDuty EKS Protection fornece detecção de ameaças em tempo de execução para seus clusters Amazon EKS no AWS ambiente. Agora é compatível com a região Ásia-Pacífico (Melbourne).	8 de agosto de 2023
Atualizou a lista de GuardDuty descobertas que invocam a verificação GuardDuty de malware iniciada	Certos tipos de descoberta do EKS Runtime Monitoring agora podem invocar uma verificação de GuardDuty malware iniciada em seu. Conta da AWS	19 de julho de 2023

GuardDuty suporta 10.000 contas de membros por meio de AWS Organizations	Agora, uma conta de GuardDuty administrador pode gerenciar no máximo 10.000 contas de membros por meio de AWS Organizations. Isso também inclui um máximo de 5000 contas de membros associadas à conta de GuardDuty administrador por convite.	29 de junho de 2023
O Monitoramento de runtime do EKS anuncia três novos tipos de descoberta.	O Monitoramento de runtime do EKS oferece suporte a três novos tipos de descoberta baseados na técnica de injeção de processo. Os novos tipos de descoberta são:Runtime/ DefenseEvasion .Proc ,:Runtime/ ProcessInjection .Ptrace e:Runtime/. DefenseEvasion ProcessInjection DefenseEvasion ProcessInjection VirtualMemoryWrite.	22 de junho de 2023
O Monitoramento de runtime do EKS lançou o novo agente v1.2.0 que suporta a versão 1.27 do Kubernetes	O EKS Runtime Monitoring lançou uma nova versão 1.2.0 do agente que também oferece suporte a instâncias baseadas em ARM64. Foi adicionado suporte para Bottlerocket. Para obter mais informações, consulte o Histórico de versões do agente complementar do EKS.	16 de junho de 2023

GuardDuty O console fornece uma visão resumida de suas descobertas.	O painel de resumo no GuardDuty console fornece uma visão agregada das GuardDuty descobertas. Atualmente, o painel exibe dados por meio de vários widgets das últimas 10.000 descobertas geradas para sua conta (ou contas de membros, se você for uma conta de GuardDuty administrador) para a região atual.	12 de junho de 2023
O Monitoramento de logs de auditoria do EKS está disponível na Ásia-Pacífico (Hyderabad), Ásia-Pacífico (Melbourne), Ásia-Pacífico (Melbourne), Europa (Zurique) e Europa (Espanha)	Habilite o Monitoramento de logs de auditoria do EKS (na Proteção do EKS) para que suas contas monitorem os logs de auditoria do Kubernetes dos seus clusters do Amazon EKS e analise-os em busca de atividades potencialmente mal-intencionadas e suspeitas.	1.º de junho de 2023
O Monitoramento de logs de auditoria do EKS está disponível no Oriente Médio (EAU)	O EKS Audit Log Monitoring agora está disponível no Oriente Médio (EAU). Habilite o Monitoramento de logs de auditoria do EKS para que suas contas monitorem os logs de auditoria do Kubernetes dos seus clusters do Amazon EKS e analise-os em busca de atividades potencialmente mal-intencionadas e suspeitas.	3 de maio de 2023

GuardDuty Malware Protection anuncia verificação de malware sob demanda	A Proteção contra malware ajuda a detectar a possível presença de malware nos volumes do Amazon EBS anexados às suas instâncias do Amazon EC2 e às workloads de contêineres. Agora, ele oferece dois tipos de escaneamentos: GuardDuty iniciados e sob demanda. GuardDuty- a verificação de malware iniciada inicia automaticamente uma verificação sem agente nos volumes do Amazon EBS somente quando GuardDuty gera uma das descobertas que invocam a verificação de malware iniciada. GuardDuty Você pode iniciar uma verificação de malware sob demanda para instâncias do Amazon EC2 em sua conta fornecendo o nome do recurso da Amazon (ARN) associado a essa instância do Amazon EC2. Para obter mais informações sobre como os dois tipos de verificação diferem, consulte Proteção contra malware. • GuardDuty- verificação de malware iniciada • Verificação de malware sob demanda	27 de abril de 2023

GuardDuty anuncia a Proteção Lambda	A Proteção do Lambda ajuda você a identificar possíveis ameaças à segurança em suas funções do AWS Lambda . • Tipos de descoberta do Lambda Protection • Correção de uma função Lambda potencialmente comprometida	20 de abril de 2023
GuardDuty agora está disponível na região Ásia-Pacífico (Melbourne)	Foi adicionada a região Ásia-Pacífico (Melbourne) à lista de Regiões da AWS onde GuardDuty está disponível. Para obter informações sobre quais recursos estão disponíveis na região, consulte Regiões e endpoints.	19 de abril de 2023

GuardDuty adicionou 3 novos tipos de descobertas do EC2	GuardDuty apresenta novos tipos de descoberta para detectar o uso de resolvedores de DNS externos e tecnologias de DNS criptografadas. Para obter informações sobre Regiões da AWS onde esses tipos de descoberta são compatíveis, consulte Regiões e endpoints. • DefenseEvasion:EC2/UnusualDNSResolver • DefenseEvasion:EC2/UnusualDoHActivity • DefenseEvasion:EC2/UnusualDoTActivity	5 de abril de 2023

GuardDuty anuncia o EKS Runtime Monitoring na EKS Protection	O EKS Runtime Monitoring dentro do EKS Protection fornece detecção de ameaças em tempo de execução para seus clusters Amazon EKS no AWS ambiente. Ele usa um agente complementar do Amazon EKS (`aws-guardduty-agent`) que coleta eventos de runtime de suas workloads do EKS. Depois de GuardDuty receber esses eventos de tempo de execução, ele os monitora e analisa para identificar possíveis ameaças suspeitas à segurança. Para obter mais informações, consulte Como encontrar detalhes e Tipos de descoberta do Monitoramento de runtime do EKS.	30 de março de 2023

GuardDuty adiciona uma nova funcionalidade — `autoEnableOrganizationMembers`	GuardDuty A Amazon adiciona uma nova opção de configuração organizacional que ajuda as contas GuardDuty do administrador a auditar e aplicar (se necessário) o que GuardDuty está habilitado para `ALL` os membros de sua organização. A prática recomendada agora é usar `autoEnableOrganizationMembers` em vez de `autoEnable` . `autoEnable` está obsoleto, mas ainda é compatível. As seguintes APIs são afetadas por essa nova funcionalidade: • DescribeOrganizationConfiguration • UpdateOrganizationConfiguration • DisassociateMembers • DeleteMembers • DisassociateFromAdministratorAccount • StopMonitoringMembers	23 de março de 2023

O recurso RDS Protection na Amazon agora GuardDuty está disponível ao público em geral	GuardDuty O RDS Protection monitora e traça o perfil da atividade de login do RDS para identificar comportamentos suspeitos de login em suas instâncias de banco de dados Amazon Aurora. Para obter informações sobre quais Regiões da AWS oferecem suporte à Proteção do RDS, consulte Regiões e endpoints.	16 de março de 2023
GuardDuty anuncia a ativação do recurso	Historicamente, a GuardDuty API permitia a configuração de recursos e fontes de dados, mas agora, todos os novos tipos de GuardDuty proteção serão configurados como recursos e não como fontes de dados. GuardDuty ainda oferece suporte às fontes de dados via API, mas não adicionará uma nova API. A ativação de recursos afeta o comportamento das APIs usadas para habilitar GuardDuty ou um tipo de proteção dentro GuardDuty delas. Se você gerencia suas GuardDuty contas por meio de um modelo de API, SDK ou CFN, consulte as alterações GuardDuty da API em março de 2023.	16 de março de 2023

GuardDuty A proteção contra malware agora está disponível na região do Oriente Médio (EAU)	O recurso de proteção contra malware GuardDuty é suportado na região do Oriente Médio (EAU). Para obter mais informações, consulte Regiões e endpoints da .	13 de março de 2023
A Amazon GuardDuty atualizou a função vinculada ao serviço (SLR)	GuardDuty adicionou as seguintes novas permissões para oferecer suporte ao próximo recurso de monitoramento de tempo de execução do GuardDuty EKS. • Use as ações do Amazon EKS para gerenciar e recuperar informações sobre os clusters do EKS e gerenciar os complementos do EKS nos clusters do EKS. As ações do EKS também recuperam as informações sobre as tags associadas a. GuardDuty `"eks:ListClusters", "eks:DescribeCluster", "ec2:DescribeVpcEndpointServices", "ec2:DescribeSecurityGroups"`	8 de março de 2023

A Amazon GuardDuty atualizou a função vinculada ao serviço (SLR)	A GuardDuty SLR foi atualizada para permitir a criação da SLR de Proteção contra Malware após a ativação da Proteção contra Malware.	21 de fevereiro de 2023
GuardDuty requer TLS v1.2 ou posterior	Para se comunicar com AWS os recursos, GuardDuty requer e oferece suporte ao TLS v1.2 ou posterior. Para obter mais informações, consulte Proteção de dados e Segurança da infraestrutura.	14 de fevereiro de 2023
GuardDuty agora está disponível na região Ásia-Pacífico (Hyderabad)	Foi adicionada a região Ásia-Pacífico (Hyderabad) à lista de Regiões da AWS onde GuardDuty está disponível. Para obter mais informações, consulte Regiões e endpoints da .	14 de fevereiro de 2023
O Amazon GuardDuty User Guide está alinhado com as melhores práticas do IAM	Guia atualizado para alinhamento com as práticas recomendadas do IAM. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM.	10 de fevereiro de 2023
GuardDuty agora está disponível na região Europa (Espanha)	A Europa (Espanha) foi adicionada à lista de Regiões da AWS onde GuardDuty está disponível. Para obter mais informações, consulte Regiões e endpoints da .	8 de fevereiro de 2023

GuardDuty agora está disponível na região Europa (Zurique)	A Europa (Zurique) foi adicionada à lista de Regiões da AWS onde GuardDuty está disponível. Para obter mais informações, consulte Regiões e endpoints da .	12 de dezembro de 2022
Versão prévia de um novo recurso — Proteção GuardDuty RDS	GuardDuty O RDS Protectio n monitora e traça o perfil da atividade de login do RDS para identificar comportam entos suspeitos de login em suas instâncias de banco de dados Amazon Aurora. Atualmente, ela está disponíve l para uma versão prévia em cinco Regiões da AWS. Para obter mais informações, consulte Regiões e endpoints da .	30 de novembro de 2022
GuardDuty agora está disponível na região do Oriente Médio (EAU)	O Oriente Médio (EAU) foi adicionado à lista de Regiões da AWS onde GuardDuty está disponível. Para obter mais informações, consulte Regiões e endpoints da .	6 de outubro de 2022

Conteúdo adicionado para um novo recurso — Proteção contra GuardDuty malware	GuardDuty A proteção contra malware é um aprimoramento opcional da Amazon GuardDuty. Enquanto GuardDuty identifica os recursos em risco, o Malware Protection detecta o malware que pode ser a fonte do comprometimento. Com a Proteção contra Malware ativada, sempre que GuardDuty detecta comportamento suspeito em uma instância do Amazon EC2 ou em uma carga de trabalho de contêiner indicativa de malware GuardDuty , a Proteção contra Malware inicia uma verificação sem agente nos volumes do EBS anexados às cargas de trabalho da instância ou contêiner do EC2 impactadas para detectar a presença de malware. Para obter informações sobre como a Proteção contra Malware funciona e como configurar esse recurso, consulte Proteção contra GuardDuty Malware. • Para obter informações sobre as descobertas da Proteção contra malware, consulte Como encontrar detalhes.	26 de julho de 2022

	• Para obter informações sobre como remediar a instância EC2 comprometida e um contêiner autônomo, consulte Correção de problemas de segurança descobertos por. GuardDuty • Para obter informações sobre CloudWatch registros de auditoria para escaneamento de malware e motivos para ignorar um recurso durante o escaneamento de malware, consulte Entendendo CloudWatch registros e motivos para ignorar. • Para obter informações sobre detecções de ameaças de falsos positivos, consulte Relatar falsos positivos na Proteção GuardDuty contra Malware.	
Um tipo de descoberta foi retirado	Exfiltration:S3/ObjectRead.Unusual foi retirado.	5 de julho de 2022

Foram adicionados novos tipos de descoberta do S3 que identificam comportamentos anômalos usando o modelo de aprendizado GuardDuty de máquina (ML) de detecção de anomalias.	Foram adicionados os novos tipos de descoberta do S3 a seguir. Esses tipos de descoberta identificam se uma solicitação de API invocou uma entidade do IAM de forma anômala. O modelo de ML avalia todas as solicitações de API em sua conta e identifica eventos anômalos associados às técnicas usadas pelos adversários. Para saber mais sobre cada uma dessas novas descobertas, consulte Tipos de descoberta do S3. • Discovery:S3/AnomalousBehavior • Impact:S3/AnomalousBehavior.Write • Impact:S3/AnomalousBehavior.Delete • Impact:S3/AnomalousBehavior.Permission • Exfiltration:S3/AnomalousBehavior	5 de julho de 2022

Conteúdo de proteção GuardDuty EKS adicionado para GuardDuty	GuardDuty Agora você pode gerar descobertas para seus recursos do Amazon EKS por meio do monitoramento dos registros de auditoria do Kubernetes. Para saber como configurar esse recurso, consulte Proteção EKS na Amazon GuardDuty. Para obter uma lista das descobertas que GuardDuty podem ser geradas para os recursos do Amazon EKS, consulte as descobertas do Kubernetes. Uma nova orientação de remediação foi adicionada para apoiar a remediação dessas descobertas no guia de descoberta de remediação do Kubernetes.	25 de janeiro de 2022
Foi adicionada 1 nova descoberta	Uma nova descoberta, UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS, foi adicionada. Essa descoberta informa quando suas credenciais de instância são acessadas por uma AWS conta fora do seu AWS ambiente.	20 de janeiro de 2022

Os tipos de descoberta foram atualizados para ajudar a identificar problemas relacionados ao log4j	A Amazon GuardDuty atualizou os seguintes tipos de descoberta para ajudar a identificar e priorizar problemas relacionados ao CVE-2021-44228 e ao CVE-2021-45046: Backdoor: EC2/C&CActivity.b; Backdoor: EC2/C&CAtivity.B! DNS; Comportamento: EC2/NetworkPortUnusual.	22 de dezembro de 2021
Alterações em descobertas	UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration foi alterado para UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS. Essa versão aprimorada da descoberta aprende os locais típicos em que suas credenciais são usadas para reduzir as descobertas do tráfego roteado por meio de redes locais. UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS	7 de setembro de 2021
Atualização para GuardDuty SLR	A GuardDuty SLR foi atualizada com novas ações para melhorar a precisão da localização.	3 de agosto de 2021

Foram adicionadas informações da fonte de dados para cada tipo de descoberta.	As descrições das descobertas agora contêm informações sobre as fontes de dados GuardDuty usadas para gerar essa descoberta.	10 de maio de 2021
Retirados 13 tipos de descobertas.	13 descobertas foram retiradas para serem substituídas por novas Anomalous Behavoir descobertas. Persistence:IAMUser/NetworkPermissions, Persistence:IAMUser/ResourcePermissions, Persistence:IAMUser/UserPermissions, PrivilegeEscalation:IAMUser/AdministrativePermissions, Recon:IAMUser/NetworkPermissions, Recon:IAMUser/ResourcePermissions, Recon:IAMUser/UserPermissions, ResourceConsumption:IAMUser/ComputeResources, Stealth:IAMUser/LoggingConfigurationModified, Discovery:S3/BucketEnumeration.Unusual, Impact:S3/ObjectDelete.Unusual, Impact:S3/PermissionsModification.Unusual.	12 de março de 2021

Foram adicionados 8 novos tipos de descoberta para comportamento anômalo.	Foram adicionados 8 novos tipos de descoberta IAMUser com base no comportamento anômalo dos diretores do IAM. CredentialAccess:IAMUser/AnomalousBehavior, DefenseEvasion:IAMUser/AnomalousBehavior, Discovery:IAMUser/AnomalousBehavior, Exfiltration:IAMUser/AnomalousBehavior, Impact:IAMUser/AnomalousBehavior, InitialAccess:IAMUser/AnomalousBehavior, Persistence:IAMUser/AnomalousBehavior, PrivilegeEscalation:IAMUser/AnomalousBehavior.	12 de março de 2021
Foram adicionadas descobertas do EC2 com base na reputação do domínio.	Foram adicionados 4 novos tipos de descoberta de impacto com base na reputação do domínio. Impact:EC2/AbusedDomainRequest.Reputation , Impact:EC2/BitcoinDomainRequest.Reputation, Impact:EC2/MaliciousDomainRequest.Reputation. Também foi adicionada uma nova descoberta do EC2 para C&CActivity. Impact:EC2/SuspiciousDomainRequest.Reputation	27 de janeiro de 2021

Foram adicionados 4 novos tipos de descoberta.	Foram adicionadas 3 novas descobertas do S3 Malicious IPCaller. Discovery:S3/MaliciousIPCaller, Exfiltration:S3/MaliciousIPCaller, Impact:S3/MaliciousIPCaller. Também foi adicionada uma nova descoberta do EC2 para C&CActivity. Backdoor:EC2/C&CActivity.B	21 de dezembro de 2020
Retirou o tipo de descoberta UnauthorizedAccess:EC2/TorIPCaller.	O tipo de UnauthorizedAccess:EC2/TorIPCaller descoberta agora foi retirado do GuardDuty. Saiba mais.	1º de outubro de 2020
Foi adicionado o tipo de descoberta Impact:EC2/WinRmBruteForce.	Foi adicionada uma nova descoberta de impacto, Impact:EC2/WinRmBruteForce. Saiba mais.	17 de setembro de 2020
Foi adicionado o tipo de descoberta Impact:EC2/PortSweep.	Foi adicionada uma nova descoberta de impacto, Impact:EC2/PortSweep. Saiba mais.	17 de setembro de 2020
GuardDuty agora está disponível nas regiões da África (Cidade do Cabo) e Europa (Milão).	Foram adicionadas África (Cidade do Cabo) e Europa (Milão) à lista de AWS regiões nas quais GuardDuty está disponível. Saiba mais	31 de julho de 2020

Foram adicionados novos detalhes de uso para monitorar GuardDuty os custos.	Agora você pode usar novas métricas para consultar dados de custo de GuardDuty uso da sua conta e das contas que você gerencia. Uma nova visão geral dos custos de uso está disponível no console em https://console.aws.amazon.com/guardduty/. Informações mais detalhadas podem ser acessadas por meio da API.	31 de julho de 2020
Conteúdo adicionado cobrindo a proteção do S3 por meio do monitoramento de eventos de dados do S3 em. GuardDuty	GuardDuty O S3 Protection agora está disponível por meio do monitoramento de eventos do plano de dados do S3 como uma nova fonte de dados. Novas contas terão esse recurso habilitado automaticamente. Se você já estiver usando, GuardDuty poderá habilitar a nova fonte de dados para você ou para suas contas de membros.	31 de julho de 2020
Foram adicionadas 14 novas descobertas do S3.	Foram adicionados 14 novos tipos de descoberta do S3 ao ambiente de gerenciamento do S3 e às fontes do plano de dados.	31 de julho de 2020

Adição de suporte para descobertas do S3 e alteração de dois nomes de tipos de descobertas existentes.	GuardDuty as descobertas agora incluem mais detalhes sobre descobertas envolvendo buckets S3. Os tipos de descoberta existentes relacionados à atividade do S3 foram renomeados: Policy:IAMUser/S3BlockPublicAccessDisabled foi alterado para Policy:S3/BucketBlockPublicAccessDisabled. Stealth:IAMUser/S3ServerAccessLoggingDisabled foi alterado para Stealth:S3/ServerAccessLoggingDisabled.	28 de maio de 2020
Conteúdo adicionado para AWS Organizations integração.	GuardDuty agora se integra com administradores AWS Organizations delegados para permitir que você gerencie GuardDuty contas em sua organização. Ao definir um administrador delegado como sua conta de GuardDuty administrador, você pode habilitar GuardDuty automaticamente que qualquer membro da organização seja gerenciado pela conta de administrador delegado. Você também pode ativar GuardDuty automaticamente novas contas de AWS Organizations membros. Saiba mais.	20 de abril de 2020

Adição de conteúdo ao recurso Exportar descobertas.	Conteúdo adicionado que descreve o recurso Export Fachts do GuardDuty.	14 de novembro de 2019
Foi adicionado o tipo de descoberta UnauthorizedAccess:EC2/MetadataDNSRebind.	Foi adicionada uma nova descoberta não autorizada, UnauthorizedAccess:EC2/MetadataDNSRebind. Saiba mais.	10 de outubro de 2019
Foi adicionado o tipo de descoberta Stealth:IAMUser/S3ServerAccessLoggingDisabled.	Foi adicionada uma nova descoberta de Stealth, Stealth:IAMUser/S3ServerAccessLoggingDisabled. Saiba mais.	10 de outubro de 2019
Foi adicionado o tipo de descoberta Policy:IAMUser/S3BlockPublicAccessDisabled.	Foi adicionada uma nova descoberta de política, Policy:IAMUser/S3BlockPublicAccessDisabled. Saiba mais.	10 de outubro de 2019
Retirou o tipo de descoberta Backdoor:EC2/XORDDOS.	O tipo de Backdoor:EC2/XORDDOS descoberta agora foi retirado do GuardDuty. Saiba mais	12 de junho de 2019
Foi adicionado o tipo de descoberta PrivilegeEscalation.	O tipo de descoberta Privilege Escalation detecta quando os usuários tentam atribuir privilégios elevados e mais permissivos às suas contas. Saiba mais	14 de maio de 2019
GuardDuty agora está disponível na região da Europa (Estocolmo).	A Europa (Estocolmo) foi adicionada à lista de AWS regiões nas quais GuardDuty está disponível. Saiba mais	9 de maio de 2019

Foi adicionado um novo tipo de descoberta, Recon:EC2/PortProbeEMRUnprotectedPort.	Essa descoberta informa que uma porta sensível relacionada ao EMR em uma instância do EC2 não está bloqueada e está sendo testada ativamente. Saiba mais	8 de maio de 2019
Adicionados 5 novos tipos de descobertas que detectam se as suas instâncias do EC2 podem estar sendo usadas para ataques de negação de serviço (DoS).	Essas descobertas informam as instâncias do EC2 em seu ambiente que estão se comportando de uma forma que pode indicar que estão sendo usadas para executar ataques de negação de serviço (DoS). Saiba mais	8 de março de 2019
Foi adicionado um novo tipo de descoberta: Policy:IAMUser/RootCredentialUsage	Policy:IAMUser/RootCredentialUsagefinding type informa que suas credenciais de login do usuário root Conta da AWS estão sendo usadas para fazer solicitações programáticas aos serviços. AWS Saiba mais	24 de janeiro de 2019
O tipo de descoberta UnauthorizedAccess:IAMUser/UnusualASNCaller foi retirado	O tipo de descoberta UnauthorizedAccess:IAMUser/UnusualASNCaller foi retirado. Agora você será notificado sobre atividades invocadas de redes incomuns por meio de outros tipos de GuardDuty descoberta ativa. O tipo de descoberta gerado será baseado na categoria da API que foi invocada a partir de uma rede incomum. Saiba mais	21 de dezembro de 2018

Foram adicionados dois novos tipos de descoberta: PenTest:IAMUser/ParrotLinux e PenTest:IAMUser/PentooLinux	O tipo de descoberta PenTest:IAMUser/ParrotLinux informa que um computador executando o Parrot Security Linux está fazendo chamadas de API usando credenciais que pertencem à sua conta da AWS . O tipo de descoberta PenTest:IAMUser/PentooLinux informa que uma máquina executando o Pentoo Linux está fazendo chamadas de API usando credenciais que pertencem à sua conta da AWS . Saiba mais	21 de dezembro de 2018
Foi adicionado suporte para o tópico SNS de GuardDuty anúncios da Amazon	Agora você pode se inscrever no tópico de GuardDuty anúncios do SNS para receber notificações sobre tipos de descoberta recém-lançados, atualizações dos tipos de descoberta existentes e outras alterações de funcionalidade. As notificações estão disponíveis em todos os formatos compatíveis com o Amazon SNS. Saiba mais	21 de novembro de 2018

Foram adicionados dois novos tipos de descoberta: UnauthorizedAccess:EC2/TorClient e UnauthorizedAccess:EC2/TorRelay	UnauthorizedAccess:EC2/TorClientfinding type informa que uma instância do EC2 em seu AWS ambiente está fazendo conexões com um nó Tor Guard ou Authority . UnauthorizedAccess:EC2/TorRelayfinding type informa que uma instância do EC2 em seu AWS ambiente está fazendo conexões com uma rede Tor de uma maneira que sugere que ela está agindo como um retransmissor Tor. Saiba mais	16 de novembro de 2018
Foi adicionado um novo tipo de descoberta: CryptoCurrency:EC2/BitcoinTool.B	Essa descoberta informa que uma instância do EC2 em seu AWS ambiente está consultando um nome de domínio associado ao Bitcoin ou a outra atividade relacionada à criptomoeda. Saiba mais	9 de novembro de 2018
Foi adicionado suporte para atualizar a frequência das notificações enviadas para CloudWatch Eventos	Agora você pode atualizar a frequência das notificações enviadas aos CloudWatch Eventos para as ocorrências subsequentes das descobertas existentes. Valores possíveis são 15 minutos, 1 hora ou 6 horas (padrão). Saiba mais	9 de outubro de 2018
Adição de suporte à região	Suporte regional adicionado para AWS GovCloud (Oeste dos EUA) Saiba mais	25 de julho de 2018

Suporte adicionado para AWS CloudFormation StackSets em GuardDuty	Você pode usar o GuardDuty modelo Enable Amazon para habilitar GuardDuty simultane amente em várias contas. Saiba mais	25 de junho de 2018
Foi adicionado suporte para regras de GuardDuty arquivamento automático	Agora, os clientes podem criar regras de autoarqui vamento granulares para a supressão de descobert as. Para descobertas que correspondam a uma regra de arquivamento automátic o, marque-as GuardDuty automaticamente como arquivadas. Isso permite que os clientes se ajustem ainda mais GuardDuty para manter apenas as descobert as relevantes na tabela de descobertas atual. Saiba mais	4 de maio de 2018
GuardDuty está disponível na região Europa (Paris)	GuardDuty agora está disponível na Europa (Paris), permitindo que você amplie o monitoramento contínuo da segurança e a detecção de ameaças nessa região. Saiba mais	29 de março de 2018
Agora AWS CloudFormation é GuardDuty possível criar contas de administrador e contas de membros por meio de.	Para ter mais informaçõ es, consulte `AWS::GuardDuty::master` e `AWS::GuardDuty::member`.	6 de março de 2018

Foram adicionadas nove novas detecções de anomalias CloudTrail baseadas.	Esses novos tipos de descoberta são habilitados automaticamente GuardDuty em todas as regiões suportadas. Saiba mais	28 de fevereiro de 2018
Adicionadas três novas detecções de inteligência de ameaças (tipos de descoberta).	Esses novos tipos de descoberta são habilitados automaticamente GuardDuty em todas as regiões suportadas. Saiba mais	5 de fevereiro de 2018
Aumento do limite para contas de GuardDuty membros.	Com esta versão, você pode ter até 1000 contas de GuardDuty membros adicionadas por AWS conta (conta de GuardDuty administrador). Saiba mais	25 de janeiro de 2018
Mudanças no upload e no gerenciamento adicional de listas de IP confiáveis e listas de ameaças para contas de GuardDuty administrador e contas de membros.	Com esta versão, os usuários de GuardDuty contas de administrador podem carregar e gerenciar listas de IPs confiáveis e listas de ameaças. Usuários de GuardDuty contas de membros não podem fazer upload e gerenciar listas. As listas de IP confiáveis e as listas de ameaças enviadas pela conta do administrador são impostas à GuardDuty funcionalidade de suas contas de membros. Saiba mais	25 de janeiro de 2018

Atualizações anteriores

Alteração	Descrição	Data
Publicação inicial	Publicação inicial do Guia GuardDuty do usuário da Amazon.	28 de novembro de 2017

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.