Manual do usuário

# Amazon Inspector

# Amazon Inspector: Manual do usuário

# Table of Contents

# O que é o Amazon Inspector?

O Amazon Inspector é um serviço de gerenciamento de vulnerabilidades que verifica continuamente suas AWS cargas de trabalho em busca de vulnerabilidades de software e exposição não intencional na rede. O Amazon Inspector descobre e escaneia automaticamente instâncias do Amazon EC2 em execução, imagens de contêineres no Amazon Elastic Container Registry (Amazon ECR) AWS Lambda e funciona em busca de vulnerabilidades conhecidas de software e exposição não intencional na rede.

O Amazon Inspector cria uma descoberta quando descobre uma vulnerabilidade de software ou um problema de configuração de rede. Uma descoberta descreve a vulnerabilidade, identifica o recurso afetado, avalia a gravidade da vulnerabilidade e fornece orientação para correção. Analise as descobertas usando o console do Amazon Inspector ou visualize e processe as descobertas por meio de outros do Serviços da AWS. Para ter mais informações, consulte Noções básicas sobre descobertas no Amazon Inspector.

Tópicos



## Características do Amazon Inspector Classic

Gerencie centralmente várias contas do Amazon Inspector

Se seu AWS ambiente tiver várias contas, você poderá gerenciar centralmente seu ambiente por meio de uma única conta usando AWS Organizations. Usando essa abordagem, é possível designar uma conta como conta do administrador delegado do Amazon Inspector.

O Amazon Inspector pode ser ativado para toda a sua organização com um único clique. Além disso, você poderá automatizar a ativação do serviço para futuros membros sempre que eles ingressarem na sua organização. A conta de administrador delegado do Amazon Inspector pode gerenciar descobertas, dados e determinadas configurações para membros da organização. Isso inclui a visualização de detalhes agregados das descobertas de todas as contas dos membros, a ativação ou desativação das verificações das contas dos membros e a revisão dos recursos escaneados dentro da organização. AWS

Analise continuamente seu ambiente em busca de vulnerabilidades e exposição à rede

Com o Amazon Inspector, você não precisará programar manualmente ou configurar verificações de avaliação. O Amazon Inspector descobre e começa automaticamente a verificar seus recursos elegíveis. O Amazon Inspector continua a avaliar seu ambiente durante todo o ciclo de vida de seus recursos, verificando novamente os recursos de maneira automática em resposta a mudanças que poderiam introduzir uma nova vulnerabilidade, como: instalar um novo pacote em uma instância do EC2, instalar um patch e quando uma nova CVE (vulnerabilidade e exposição comum) que afeta o recurso é publicada. Ao contrário do software tradicional de verificação de segurança, o Amazon Inspector tem um impacto mínimo no desempenho da sua frota.

Quando vulnerabilidades ou caminhos de rede abertos são identificados, o Amazon Inspector produz uma descoberta que é possível investigar. A descoberta inclui detalhes abrangentes sobre a vulnerabilidade, o recurso afetado e recomendações de correção. Se corrigir adequadamente uma descoberta, o Amazon Inspector detecta automaticamente a correção e fecha a descoberta.

Avaliar as vulnerabilidades com precisão com a pontuação de risco do Amazon Inspector

Como o Amazon Inspector coleta informações sobre seu ambiente por meio de verificações, ele fornece pontuações de severidade especificamente adaptadas ao seu ambiente. O Amazon Inspector examina as métricas de segurança que compõem a pontuação base do NVD (Banco de dados nacional de vulnerabilidades) para uma vulnerabilidade e as ajusta de acordo com seu ambiente de computação. Por exemplo, o serviço pode diminuir a pontuação do Amazon Inspector de uma descoberta para uma instância do Amazon EC2 se a vulnerabilidade for explorável pela rede, mas nenhum caminho de rede aberto para a internet estiver disponível na instância. Essa pontuação está no formato CVSS e é uma modificação da pontuação básica do CVSS (Sistema comum de pontuação de vulnerabilidade) fornecida pelo NVD.

Identifique descobertas de alto impacto com o painel do Amazon Inspector

O painel do Amazon Inspector oferece uma visão de alto nível das descobertas de todo o seu ambiente. No painel, é possível acessar detalhes granulares de uma descoberta. O painel contém informações simplificadas sobre a cobertura de verificação em seu ambiente, suas descobertas mais importantes e quais recursos têm mais descobertas. O painel de correção baseado em riscos no painel do Amazon Inspector apresenta as descobertas que afetam o maior número de instâncias e imagens. Esse painel facilita a identificação das descobertas com maior impacto em seu ambiente, a análise dos detalhes das descobertas e a análise das soluções sugeridas.

Gerencie suas descobertas usando visualizações personalizáveis

Além do painel, o console do Amazon Inspector oferece uma visualização das Descobertas. Esta página lista todas as descobertas do seu ambiente e fornece os detalhes das descobertas

individuais. Visualize as descobertas agrupadas por categoria ou tipo de vulnerabilidade. Em cada visualização, personalize ainda mais seus resultados usando filtros. Você também poderá usar filtros para criar regras de supressão que ocultem descobertas indesejadas de suas visualizações.

Use os filtros e regras de supressão para gerar relatórios de descobertas que mostrem todas as descobertas ou uma seleção personalizada das descobertas. Os relatórios podem ser gerados nos formatos CSV ou JSON.

Monitore e processe as descobertas com outros serviços e sistemas

Para apoiar a integração com outros serviços e sistemas, o Amazon Inspector publica descobertas na Amazon EventBridge como eventos de descoberta. EventBridge é um serviço de barramento de eventos sem servidor que pode encaminhar dados de descobertas para destinos como AWS Lambda funções e tópicos do Amazon Simple Notification Service (Amazon SNS). Com EventBridge, você pode monitorar e processar as descobertas quase em tempo real como parte de seus fluxos de trabalho existentes de segurança e conformidade.

Se você tiver ativado AWS Security Hub, o Amazon Inspector também publicará as descobertas no Security Hub. O Security Hub é um serviço que fornece uma visão abrangente de sua postura de segurança em todo o AWS ambiente e ajuda você a verificar seu ambiente de acordo com os padrões e as melhores práticas do setor de segurança. Com o Security Hub, é possível monitorar e processar com mais facilidade as descobertas como parte de uma análise mais ampla do procedimento de segurança da organização na AWS.

# Acessar o Amazon Inspector

O Amazon Inspector está disponível na maioria. Regiões da AWS Para obter uma lista de regiões onde o Amazon Inspector está disponível atualmente, consulte os Endpoints e cotas do Amazon Inspector na Referência geral do Amazon Web Services. Para saber mais sobre as Regiões da AWS, consulte Gerenciamento das Regiões da AWS na Referência geral da Amazon Web Services. É possível trabalhar com o Amazon Inspector das seguintes maneiras indicadas a seguir em cada região.

AWS Console de Gerenciamento

AWS Management Console É uma interface baseada em navegador que você pode usar para criar e gerenciar AWS recursos. Como parte desse console, o console do Amazon Inspector fornece acesso à sua conta e recursos do Amazon Inspector. Execute as tarefas do Amazon Inspector no console do Amazon Inspector.

### AWS ferramentas de linha de comando

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

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

### AWS SDKs

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

### API REST do Amazon Inspector

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

# Conceitos básicos do Amazon Inspector

Este tutorial fornece uma apresentação prática ao Amazon Inspector.

A etapa 1 abrange a ativação de escaneamentos do Amazon Inspector para uma conta autônoma ou como administrador delegado do Amazon Inspector em um ambiente de várias contas. AWS Organizations

A etapa 2 abrange a compreensão das descobertas do Amazon Inspector no console.

> **Note**
>
> Neste tutorial, você conclui as tarefas em sua versão atual Região da AWS. Para configurar o Amazon Inspector em outras regiões, conclua essas etapas em cada uma dessas regiões.

Tópicos



## Antes de começar

O Amazon Inspector é um serviço de gerenciamento de vulnerabilidades que verifica continuamente suas instâncias do Amazon EC2, imagens de contêineres do Amazon ECR e AWS Lambda funções em busca de vulnerabilidades de software e exposição não intencional na rede.

Observe o seguinte antes de ativar o Amazon Inspector:

- O Amazon Inspector é um serviço regional e os dados são armazenados no Região da AWS local onde você usa o serviço. Qualquer um dos procedimentos de configuração que você concluir neste tutorial deve ser repetido em cada um Região da AWS que você deseja monitorar com o Amazon Inspector.
- O Amazon Inspector oferece a flexibilidade de ativar a instância do Amazon EC2, a imagem do contêiner do Amazon ECR e a varredura de funções. AWS Lambda Gerencie os tipos de

verificação na página de gerenciamento de contas no console do Amazon Inspector ou usando as APIs do Amazon Inspector.

- O Amazon Inspector pode fornecer dados de CVE (vulnerabilidades e exposições comuns) para suas instâncias do EC2 somente se o atendente do SSM (Gerenciador de Sistemas) do Amazon EC2 estiver instalado e ativado. Esse atendente está pré-instalado em muitas instâncias do EC2, mas talvez seja necessário ativá-lo manualmente. Independentemente do status do atendente do SSM, todas as suas instâncias do EC2 são verificadas em busca de problemas de exposição na rede. Para obter mais informações sobre como configurar verificações para o Amazon EC2, consulte o Verificar as instâncias do Amazon EC2. O Amazon ECR e o escaneamento de AWS Lambda funções não exigem o uso de um agente.
- Uma identidade de usuário do IAM com permissões de administrador em um Conta da AWS pode habilitar o Amazon Inspector. Para fins de proteção de dados, recomendamos que você proteja suas 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 gerenciar o Amazon Inspector. Para obter informações sobre as permissões necessárias para habilitar o Amazon Inspector, consulte AWS política gerenciada: AmazonInspector2FullAccess.
- Ao ativar o Amazon Inspector pela primeira vez em qualquer região, ele cria uma função vinculada ao serviço globalmente para sua conta chamada `AWSServiceRoleForAmazonInspector2`. Essa função inclui as permissões e as políticas de confiança que permitem ao Amazon Inspector coletar detalhes do pacote de software e analisar as configurações do Amazon VPC para gerar descobertas de vulnerabilidade. Para ter mais informações, consulte Uso de funções vinculadas a serviço para o Amazon Inspector. Para obter mais informações sobre as funções vinculadas a um serviço, consulte Como usar funções vinculadas a serviços.

# Etapa 1: ativar o Amazon Inspector

O primeiro passo para usar o Amazon Inspector é ativá-lo para sua Conta da AWS. Depois de ativar qualquer tipo de verificação do Amazon Inspector, o Amazon Inspector imediatamente começa a descobrir e verificar todos os recursos elegíveis.

Se você quiser gerenciar o Amazon Inspector para várias contas dentro da sua organização por meio de uma conta de administrador centralizada, você deverá designar um administrador delegado para o Amazon Inspector. Escolha uma das opções a seguir para aprender como ativar o Amazon Inspector para seu ambiente.

Standalone account environment

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. Selecione a opção Conceitos básicos.
3. Escolha Ativar o Amazon Inspector.

Ao ativar o Amazon Inspector em uma conta independente, todos os tipos de verificação são ativados por padrão. Gerencie os tipos de verificação ativados na página de gerenciamento de contas no console do Amazon Inspector ou usando as APIs do Amazon Inspector. Depois que o Amazon Inspector é ativado, ele automaticamente descobre e começa a verificar todos os recursos elegíveis. Analise as seguintes informações sobre o tipo de verificação para entender quais recursos são elegíveis por padrão:

Verificar o Amazon EC2

Para fornecer dados de Vulnerabilidades e Exposições Comuns (CVE) para sua instância EC2, o Amazon Inspector exige que o agente do Systems AWS Manager (SSM) seja instalado e ativado. Esse atendente vem pré-instalado em muitas instâncias do EC2, mas talvez seja necessário ativá-lo manualmente. Independentemente do status do atendente do SSM, todas as suas instâncias do EC2 serão verificadas em busca de problemas de exposição na rede. Para obter mais informações sobre como configurar verificações para o Amazon EC2, consulte o Verificar as instâncias do Amazon EC2 com o Amazon Inspector.

Verificação do Amazon ECR

Ao ativar o escaneamento do Amazon ECR, o Amazon Inspector converte todos os repositórios de contêineres em seu registro privado que estão configurados para o Escaneamento básico padrão fornecido pelo Amazon ECR em Escaneamento avançado com escaneamento contínuo. Outra opção é definir essa configuração para verificar somente por push ou para verificar repositórios selecionados por meio de regras de inclusão. Todas as imagens enviadas nos últimos 30 dias estão programadas para verificação Vitalícia. Essa configuração de escaneamento do ECR do Amazon pode ser alterada a qualquer momento. Para obter mais informações sobre a configuração de verificações do Amazon ECR, consulte Verificar imagens de contêineres do Amazon ECR com o Amazon Inspector.

### AWS Lambda varredura de funções

Quando você ativa a verificação de AWS Lambda funções, o Amazon Inspector descobre as funções do Lambda em sua conta e imediatamente começa a escaneá-las em busca de vulnerabilidades. O Amazon Inspector verifica novas funções do Lambda e camadas quando elas são implantadas e as examina novamente quando são atualizadas ou quando novas CVEs (vulnerabilidades e exposições comuns) são publicadas. O Amazon Inspector oferece dois níveis diferentes de escaneamento da função do Lambda. Por padrão, ao ativar o Amazon Inspector pela primeira vez, a escaneamento padrão do Lambda é ativado, que verifica as dependências do pacote em suas funções. Além disso, você poderá ativar o escaneamento de código do Lambda para verificar o código do desenvolvedor em suas funções em busca de vulnerabilidades de código. Para obter mais informações sobre como configurar a verificação da função do Lambda, consulte o AWS Lambda Funções de digitalização com o Amazon Inspector.

## Multi-account environment

**Important**

Para concluir essas etapas, é necessário estar na mesma organização de todas as contas que deseja gerenciar e ter acesso à conta de gerenciamento do AWS Organizations para delegar um administrador para o Amazon Inspector em sua organização. Permissões adicionais podem ser necessárias para delegar um administrador. Para ter mais informações, consulte Permissões necessárias para designar um administrador delegado.

**Note**

Para habilitar programaticamente o Amazon Inspector para várias contas em várias regiões, use um script de shell desenvolvido pelo Amazon Inspector. Para obter mais informações sobre como usar esse script, consulte o inspetor2-enablement-with-cli on. GitHub

### Delegar um administrador do Amazon Inspector

1. Faça login na conta AWS Organizations de gerenciamento.

2. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
3. No painel Administrador delegado, insira o ID de doze dígitos do Conta da AWS que você deseja designar como administrador delegado do Amazon Inspector para a organização. Em seguida, selecione Excluir. Em seguida, na janela de confirmação, selecione Delegar novamente.

> **Note**
>
> O Amazon Inspector é ativado para sua conta ao delegar um administrador.

### Adicionar contas-membro

Como administrador delegado, ative a verificação de qualquer membro associado à conta de gerenciamento do Organizações. Esse fluxo de trabalho ativa todos os tipos de verificação para todas as contas dos membros. No entanto, os membros também podem ativar o Amazon Inspector para suas próprias contas, ou as verificações de um serviço podem ser ativadas seletivamente pelo administrador delegado. Para ter mais informações, consulte Gerenciar várias contas.

1. Faça login na conta de administrador delegada.
2. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
3. No painel de navegação, selecione Gerenciamento de contas. A tabela Contas exibe todas as contas de membros associadas à conta de gerenciamento do Organizações.
4. Na página Gerenciamento de contas, você pode escolher Ativar escaneamento para todas as contas no banner superior para ativar instâncias do EC2, imagens de contêiner ECR e escaneamento de AWS Lambda funções para todas as contas em sua organização. Como alternativa, escolha as contas que deseja adicionar como membros selecionando-as na tabela Contas. Em seguida, no menu Ativar, selecione Todas as verificações.
5. (Opcional) Ative o recurso Ativar automaticamente o Inspetor para novas contas de membros e selecione os tipos de verificação a serem incluídos para ativar esses escaneamentos para quaisquer novas contas de membros que sejam adicionadas à sua organização.

Atualmente, o Amazon Inspector oferece escaneamentos para instâncias EC2, imagens de contêineres ECR e funções. AWS Lambda Depois de ativar o Amazon Inspector, ele automaticamente começa a descobrir e escanear todos os recursos elegíveis. Analise as seguintes informações sobre o tipo de escaneamento para entender quais recursos são elegíveis por padrão:

Verificar o Amazon EC2

Para fornecer dados de vulnerabilidade CVE para suas instâncias EC2, o Amazon Inspector exige que o agente do Systems AWS Manager (SSM) seja instalado e ativado. Esse atendente vem pré-instalado em muitas instâncias do EC2, mas talvez seja necessário ativá-lo manualmente. Independentemente do status do atendente do SSM, todas as suas instâncias do EC2 serão verificadas em busca de problemas de exposição na rede. Para obter mais informações sobre como configurar verificações para o Amazon EC2, consulte o Verificar as instâncias do Amazon EC2 com o Amazon Inspector.

Escaneamento do Amazon ECR

Ao ativar o escaneamento do Amazon ECR, o Amazon Inspector converte todos os repositórios de contêineres em seu registro privado que estão configurados para o Escaneamento básico padrão fornecido pelo Amazon ECR em Escaneamento avançado com verificação contínua. Opcionalmente, você também pode definir essa configuração para verificar somente por push ou para verificar repositórios selecionados por meio de regras de inclusão. Todas as imagens enviadas nos últimos 30 dias estão programadas para verificação Vitalícia. Essa configuração de escaneamento do Amazon ECR pode ser alterada pelo administrador delegado a qualquer momento. Para obter mais informações sobre a configuração de verificações do Amazon ECR, consulte Verificar imagens de contêineres do Amazon ECR com o Amazon Inspector.

AWS Lambda varredura de funções

Quando você ativa a verificação de AWS Lambda funções, o Amazon Inspector descobre as funções do Lambda em sua conta e imediatamente começa a escaneá-las em busca de vulnerabilidades. O Amazon Inspector verifica novas funções do Lambda e camadas do quando elas são implantadas e as examina novamente quando são atualizadas ou quando novas CVEs (vulnerabilidades e exposições comuns) são publicadas. Para obter mais informações sobre como configurar a verificação da função do Lambda, consulte o AWS Lambda Funções de digitalização com o Amazon Inspector.

# Etapa 2: visualizar descobertas do Amazon Inspector

Visualize as descobertas do seu ambiente no console do Amazon Inspector ou por meio da API. Todas as descobertas também são enviadas para a Amazon EventBridge e AWS Security Hub (se ativadas). Além disso, as descobertas de imagens de contêineres são enviadas ao Amazon ECR.

O console do Amazon Inspector oferece vários formatos de visualização diferentes para suas descobertas. O painel do Amazon Inspector oferece uma visão geral de alto nível dos riscos para o seu ambiente, enquanto a tabela Descobertas permite visualizar os detalhes de uma descoberta específica.

Nesta etapa, você explora os detalhes de uma descoberta usando a tabela Descobertas e o painel Descobertas. Para obter informações sobre o painel do Amazon Inspector, consulte Noções básicas sobre o painel.

Para ver detalhes das descobertas do seu ambiente no console do Amazon Inspector:

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. No painel de navegação, selecione Painel. Selecione qualquer um dos links no painel para navegar até uma página no console do Amazon Inspector com mais detalhes sobre esse item.
3. No painel de navegação, selecione Descobertas.
4. Por padrão, você verá a guia Todas as descobertas, que exibe todas as descobertas da instância EC2, do contêiner do ECR e das AWS Lambda funções do seu ambiente.
5. Na lista Descobertas, escolha um nome de descoberta na coluna Título para abrir o painel de detalhes dessa descoberta. Todas as descobertas têm uma guia Detalhes da descoberta. Interaja com o guia Detalhes da descoberta das seguintes formas:

   - Para ver mais informações sobre vulnerabilidade, siga o link na seção Detalhes da vulnerabilidade para abrir a documentação dessa vulnerabilidade.
   - Para investigar melhor seu recurso, siga o link ID do recurso na seção Recurso afetado para abrir o console de serviço do recurso afetado.

   As descobertas do tipo de vulnerabilidade do package também têm uma Pontuação do Inspector e uma guia de inteligência de vulnerabilidade explicando como a pontuação do Amazon Inspector foi calculada para essa descoberta e fornecendo informações sobre as CVEs (vulnerabilidades e explorações comuns) associadas à descoberta. Para obter mais detalhes sobre tipos de descoberta, consulte o Tipos de descoberta no Amazon Inspector.

# Noções básicas sobre o painel do Amazon Inspector

O painel do Amazon Inspector fornece um instantâneo das estatísticas agregadas de seus AWS recursos na região atual. AWS Essas estatísticas incluem métricas-chave para cobertura de recursos e vulnerabilidades ativas. O painel também exibe grupos de dados agregados de descobertas da sua conta, como instâncias do Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Registry (Amazon ECR) e funções com as descobertas mais importantes. AWS Lambda Para realizar uma análise mais profunda, visualize os dados de suporte dos itens do painel.

Se sua conta for a conta de administrador delegado do Amazon Inspector para uma organização, o painel inclui cobertura da conta, estatísticas agregadas e dados de descobertas para todas as contas em sua organização, incluindo sua própria conta.

## Noções básicas sobre o painel

O painel mostra uma visão geral da cobertura do seu ambiente e das descobertas críticas.

Para exibir o painel:

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. No painel de navegação, escolha Painel.
3. Você poderá interagir com o painel das seguintes maneiras:

    - O painel é atualizado automaticamente a cada cinco minutos. No entanto, é possível atualizar os dados manualmente selecionando o ícone de atualização no canto superior direito da página.
    - Para visualizar os dados de suporte de um item no painel, escolha o item.
    - Se você gerencia várias contas por meio de AWS organizações como administrador delegado do Amazon Inspector, o painel exibirá estatísticas agregadas para suas contas de membros. Para filtrar o painel e exibir dados apenas para uma específica conta, insira o ID da conta na caixa Conta.

# Noções básicas sobre os componentes do painel e interpretar os dados

Cada seção do painel do Amazon Inspector fornece informações sobre as principais métricas ou dados de descobertas ativas que podem ajudá-lo a entender a postura de vulnerabilidade de seus recursos AWS na atual Região da AWS.

Cobertura ambiental

A seção de Cobertura ambiental fornece estatísticas sobre os recursos verificados pelo Amazon Inspector. Nesta seção, você pode ver a contagem e a porcentagem de instâncias do Amazon EC2, imagens e AWS Lambda funções do Amazon ECR digitalizadas pelo Amazon Inspector. Se você gerenciar várias contas AWS Organizations como administrador delegado do Amazon Inspector, você também verá o número total de contas da organização, o número com o Amazon Inspector ativado e a porcentagem de cobertura resultante para a organização. Você também poderá usar esta seção para definir quais recursos não são cobertos pelo Amazon Inspector. Esses recursos podem conter vulnerabilidades que podem ser exploradas para colocar sua organização em risco. Para obter mais detalhes, consulte Avaliar a cobertura do Amazon Inspector sobre seu ambiente da AWS.

A escolha de um grupo de cobertura leva você à página Gerenciamento de contas do agrupamento selecionado. A página de gerenciamento de contas mostra detalhes sobre quais contas, instâncias do Amazon EC2 e repositórios do Amazon ECR são cobertos pelo Amazon Inspector.

Estão disponíveis os seguintes grupos de cobertura:

- Conta
- Instâncias
- Repositórios de contêineres
- Imagens de contêiner
- Lambda

Descobertas críticas

A seção Descobertas críticas fornece uma contagem das vulnerabilidades críticas em seu ambiente e uma contagem total de todas as descobertas em seu ambiente. Nesta seção, as contagens são mostradas por recurso e tipo de avaliação. Para obter mais informações sobre

descobertas críticas e como o Amazon Inspector determina o caráter crítico, consulte Noções básicas sobre descobertas no Amazon Inspector.

A escolha de um grupo de descobertas críticas leva você à página Todas as descobertas e aplica filtros automaticamente para mostrar todas as descobertas críticas que correspondem ao agrupamento selecionado.

Os seguintes grupos de descobertas críticas estão disponíveis:

- Descobertas de imagens de contêineres do ECR
- Descobertas do Amazon EC2
- Descobertas sobre a acessibilidade da rede
- AWS Lambda descobertas da função

Correções baseadas em riscos

A seção Correções baseadas em riscos mostra os cinco principais pacotes de software com vulnerabilidades críticas que afetam a maioria dos recursos em seu ambiente. A correção desses pacotes pode reduzir significativamente o número de riscos críticos em seu ambiente. Escolha o nome do pacote de software para visualizar os detalhes da vulnerabilidade associada e os recursos afetados.

Contas com as descobertas mais importantes

A seção Contas com as descobertas mais críticas mostra as cinco principais AWS contas em seu ambiente com as descobertas mais críticas e o número total de descobertas dessa conta. Esta seção só pode ser visualizada na conta do administrador delegado quando o Amazon Inspector está configurado para digitalização de várias contas com. AWS Organizations Essa visão ajuda os administradores delegados a entender quais contas podem estar em maior risco na organização.

Escolha ID da conta para consultar mais informações sobre a conta do membro afetada.

Repositórios do Amazon ECR com as descobertas mais importantes

A seção Repositórios do Elastic Container Registry (ECR) com as descobertas mais críticas, mostra os cinco principais repositórios do Amazon ECR em seu ambiente com as descobertas mais críticas de imagens de contêineres. A exibição mostra o nome do repositório, o identificador da AWS conta, a data de criação do repositório, o número de vulnerabilidades críticas e o número total de vulnerabilidades. Essa visualização ajuda a identificar quais repositórios podem estar em maior risco.

Escolha Nome do repositório para consultar mais informações sobre o repositório afetado.

Imagens de contêiner com as descobertas mais críticas

A seção Imagens de contêiner com descobertas mais críticas mostra as cinco principais imagens de contêiner em seu ambiente com as descobertas mais críticas. A exibição mostra dados da tag de imagem, nome do repositório, resumo da imagem, identificador da AWS conta, número de vulnerabilidades críticas e número total de vulnerabilidades. Essa visualização ajuda os proprietários de aplicativos a identificar quais imagens de contêiner podem precisar ser compiladas novamente e reiniciadas.

Escolha Imagem do contêiner para consultar mais informações sobre a imagem do contêiner afetada.

Instâncias com as descobertas mais críticas

A seção Instâncias com descobertas mais críticas mostra as cinco principais instâncias do Amazon EC2 com as descobertas mais críticas. A exibição mostra o identificador da instância, o identificador da conta da AWS , o identificador da imagem de máquina da Amazon (AMI), o número de vulnerabilidades críticas e o número total de vulnerabilidades. Essa visão ajuda os proprietários da infraestrutura a identificar quais instâncias podem precisar de patches.

Escolha ID da instância para consultar mais informações sobre a instância afetada do Amazon EC2.

imagem de máquina da Amazon (AMI) com as descobertas mais críticas

A seção imagem de máquina da Amazon (AMI) com as descobertas mais críticas mostra as cinco principais AMIs em seu ambiente com as descobertas mais críticas. A exibição mostra o identificador da AMI, o identificador da conta da AWS , o número de instâncias EC2 afetadas em execução no ambiente, a data de criação da AMI, a plataforma do sistema operacional da AMI, o número de vulnerabilidades críticas e o número total de vulnerabilidades. Essa visão ajuda os proprietários da infraestrutura a identificar quais AMIs podem precisar ser compiladas novamente.

Escolha Instâncias afetadas para consultar mais informações sobre as instâncias executadas a partir da AMI afetada.

AWS Lambda funções com as descobertas mais críticas

A seção de funções do AWS Lambda com descobertas mais críticas mostra as cinco principais funções do Lambda em seu ambiente com as descobertas mais críticas. A exibição mostra o nome da função Lambda, o identificador da AWS conta, o ambiente de execução, o número de

vulnerabilidades críticas, o número de vulnerabilidades altas e o número total de vulnerabilidades. Essa visão ajuda os proprietários da infraestrutura a identificar quais funções do Lambda podem exigir correção.

Escolha Nome da função para ver mais informações sobre a AWS Lambda função afetada.

# Noções básicas sobre descobertas no Amazon Inspector

Uma descoberta é um relatório detalhado sobre uma vulnerabilidade que afeta um de seus AWS recursos. As descobertas são nomeadas de acordo com as vulnerabilidades detectadas e fornecem classificações de gravidade, informações sobre os recursos afetados e detalhes que descrevem como corrigir as vulnerabilidades relatadas.

O Amazon Inspector gera uma descoberta sempre que detecta uma vulnerabilidade em uma instância do Amazon EC2, uma imagem de contêiner em um repositório do Amazon ECR ou uma função. AWS Lambda O Amazon Inspector verifica continuamente seu ambiente computacional e armazena todas as suas descobertas ativas até que você as corrija.

Quando você corrige uma descoberta, a descoberta é fechada automaticamente e o Amazon Inspector exclui a descoberta após 7 dias. Quando você exclui um recurso, o Amazon Inspector exclui qualquer descoberta associada ao recurso após 30 dias.

Se você desativar o Amazon Inspector, as descobertas serão removidas após 24 horas. Se AWS suspender sua conta, as descobertas serão removidas após 90 dias.

As descobertas são categorizadas em um dos seguintes estados:

Ativo

O Amazon Inspector identifica descobertas que não foram corrigidas como ativas.

Suprimido

O Amazon Inspector identifica as descobertas que estão sujeitas a uma ou mais regras de supressão como Suprimidas. Você pode encontrar descobertas suprimidas na lista de descobertas suprimidas. Para ter mais informações, consulte Suprimir descobertas do Amazon Inspector com regras de supressão.

Fechado

Depois de corrigir uma vulnerabilidade, o Amazon Inspector detecta isso automaticamente e altera o estado da descoberta para Fechado. As descobertas fechadas são excluídas após 7 dias.

Tópicos

- Localizando e visualizando as descobertas do Amazon Inspector
- Detalhes da descoberta do Amazon Inspector
- Pontuação do Amazon Inspector e inteligência de vulnerabilidade
- Níveis de severidade para descobertas do Amazon Inspector

# Tipos de descoberta no Amazon Inspector

O Amazon Inspector gera descobertas para instâncias do Amazon Elastic Compute Cloud (Amazon EC2), imagens de contêineres nos repositórios e funções do Amazon Elastic Container Registry (Amazon ECR). AWS Lambda O Amazon Inspector pode gerar os seguintes tipos de descobertas.

## Vulnerabilidade do pacote

As descobertas de vulnerabilidade de pacotes identificam pacotes de software em seu AWS ambiente que estão expostos a Common Vulnerabilities and Exposures (CVEs). Os invasores podem explorar essas vulnerabilidades sem correção e comprometer a confidencialidade, a integridade ou a disponibilidade dos dados, ou para acessar outros sistemas. O sistema de CVE é um método de referência a informações conhecidas publicamente sobre vulnerabilidades e exposições de segurança. Para obter mais informações, consulte https://www.cve.org/.

As detecções de CVE para Linux são adicionadas ao Amazon Inspector dentro de 24 horas após o lançamento pelas recomendações de segurança do fornecedor. As detecções de CVE para Windows são adicionadas ao Amazon Inspector dentro de 48 horas após serem lançadas pela Microsoft. Use o Pesquisa no banco de dados de vulnerabilidades do Amazon Inspector para consultar se a detecção de CVE tem suporte.

O Amazon Inspector pode gerar descobertas de vulnerabilidade de pacotes para instâncias EC2, imagens de contêineres ECR e funções do Lambda. As descobertas de vulnerabilidade do pacote têm detalhes adicionais exclusivos para esse tipo de descoberta, como a Pontuação do inspetor e inteligência de vulnerabilidade.

## Vulnerabilidade de código

As descobertas da vulnerabilidade do código identificam linhas em seu código que os invasores poderiam explorar. As vulnerabilidades do código incluem falhas de injeção, vazamentos de dados, criptografia fraca ou criptografia ausente em seu código.

O Amazon Inspector avalia o código do seu aplicativo de função do Lambda usando raciocínio automatizado e machine learning que analisa o código do seu aplicativo para verificar a conformidade geral de segurança. Ele identifica violações de políticas e vulnerabilidades com base em detectores internos desenvolvidos em colaboração com a Amazon. CodeGuru Para obter uma lista de possíveis detecções, consulte Biblioteca de CodeGuru detectores.

> **Important**
>
> O escaneamento de código do Amazon Inspector captura trechos de código para destacar as vulnerabilidades detectadas. Esses trechos podem mostrar credenciais codificadas ou outros materiais confidenciais em texto simples.

O Amazon Inspector pode gerar descobertas de Vulnerabilidade de código para funções do Lambda se você tiver ativado o Escaneamento de código do Lambda do Amazon Inspector.

Trechos de código detectados em conexão com uma vulnerabilidade de código são armazenados pelo CodeGuru serviço. Por padrão, uma AWS chave própria controlada por CodeGuru é usada para criptografar seu código, no entanto, você pode usar sua própria chave gerenciada pelo cliente para criptografia por meio da API do Amazon Inspector. Para obter mais informações, consulte Criptografia em repouso para código em suas descobertas.

## Acessibilidade de rede

As descobertas de acessibilidade da rede indicam que há caminhos de rede abertos para instâncias do Amazon EC2 em seu ambiente. Essas descobertas aparecem quando as portas TCP e UDP são acessíveis a partir das bordas da VPC, como um gateway de internet (inclusive instâncias atrás de Application Load Balancers ou Classic Load Balancers), uma conexão de emparelhamento da VPC ou uma VPN por meio de um gateway virtual. Essas descobertas destacam configurações de rede que podem ser excessivamente permissivas, como grupos de segurança mal gerenciados, listas de controle de acesso ou gateways de internet, ou que podem permitir acesso potencialmente mal intencionados.

O Amazon Inspector gera somente descobertas de acessibilidade de rede para instâncias do Amazon EC2. O Amazon Inspector realiza verificações de descobertas de acessibilidade de rede a cada 24 horas.

O Amazon Inspector avalia as seguintes configurações ao verificar caminhos de rede:

- Instâncias do Amazon EC2
- AWS Lambda funções
- Application Load Balancers
- Conexão direta
- Elastic Load Balancers
- Interfaces de rede elástica
- Gateways da Internet
- Listas de controle de acesso à rede
- Tabelas de rotas
- Grupos de segurança
- Subredes
- Nuvens privadas virtuais
- Gateways privados virtuais
- Endpoints da VPC
- Endpoints de gateway da VPC
- Conexões de emparelhamento da VPC
- Conexões da VPN

## Localizando e visualizando as descobertas do Amazon Inspector

Os procedimentos nesta seção descrevem como localizar e visualizar descobertas no Amazon Inspector por meio do console e da API do Amazon Inspector. Os detalhes da busca variam de acordo com o tipo de descoberta, o tipo de vulnerabilidade e os recursos afetados. Para ter mais informações, consulte Detalhes da descoberta do Amazon Inspector.

Console

Para visualizar descobertas no console

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. No painel de navegação, escolha Descobertas. Você é direcionado para uma tela de descobertas, na qual pode ver todas as suas descobertas. Na tabela Descobertas, você pode escolher uma descoberta selecionando o nome da descoberta na coluna Título.

3. (Opcional) Você também pode ver as descobertas agrupadas por categoria. No painel de navegação, escolha Descobertas e, em seguida, escolha uma das seguintes categorias:

   - Por vulnerabilidade
   - Por exemplo

     > **Note**
     >
     > As descobertas agrupadas por instância não incluem informações sobre a disponibilidade da rede.

   - Por imagem de contêiner
   - Por repositório de contêineres
   - Por função Lambda

API

Execute a operação ListFindings da API. Na solicitação, você pode especificar `filterCriteria` para retornar descobertas específicas.

# Detalhes da descoberta do Amazon Inspector

No console do Amazon Inspector, visualize detalhes de cada descoberta. Os detalhes da descoberta variam com base no tipo de descoberta.

Como exibir os detalhes de uma descoberta

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home
2. Selecione a Região para visualizar as descobertas.
3. No painel de navegação, escolha Descobertas para exibir a lista de descobertas
4. (Opcional) Use a barra de filtro para selecionar uma descoberta específica. Para ter mais informações, consulte Filtrar as descobertas do Amazon Inspector.
5. Selecione uma descoberta para visualizar o painel de detalhes.

O painel Detalhes da descoberta contém os recursos básicos de identificação da descoberta. Isso inclui o título da descoberta, bem como uma descrição básica da vulnerabilidade identificada,

sugestões de correção e uma pontuação de gravidade. Para informações sobre a pontuação, consulte Níveis de severidade para descobertas do Amazon Inspector.

Os detalhes disponíveis para uma descoberta variam de acordo com o tipo de descoberta e o Recurso afetado.

Todas as descobertas contêm o número de Conta da AWS identificação pelo qual a descoberta foi identificada, uma gravidade, um tipo de descoberta, a data em que a descoberta foi criada e uma seção de recursos afetados com detalhes sobre esse recurso.

O Tipo de descoberta determina as informações de inteligência de remediação e vulnerabilidade disponíveis para a descoberta. Dependendo do tipo de descoberta, diferentes detalhes da descoberta estão disponíveis.

Vulnerabilidade do pacote

As descobertas de vulnerabilidade do pacote estão disponíveis para instâncias EC2, imagens de contêiner ECR e funções do Lambda. Consulte Vulnerabilidade do pacote para obter mais informações.

As descobertas de vulnerabilidade do pacote também incluem Pontuação do Amazon Inspector e inteligência de vulnerabilidade.

Esse tipo de descoberta tem os seguintes detalhes:

- Correção disponível: indica se a vulnerabilidade foi corrigida em uma versão mais recente dos pacotes afetados. Tem um dos seguintes valores:
  - `YES`, o que significa que todos os pacotes afetados têm uma versão fixa.
  - `NO`, o que significa que nenhum pacote afetado tem uma versão fixa.
  - `PARTIAL`, o que significa que um ou mais (mas não todos) dos pacotes afetados têm uma versão fixa.
- Exploração disponível: indica que a vulnerabilidade tem uma exploração conhecida.
  - `YES`, o que significa que a vulnerabilidade descoberta em seu ambiente tem uma exploração conhecida. O Amazon Inspector não tem visibilidade sobre o uso de explorações em um ambiente.
  - `NO`, o que significa que essa vulnerabilidade não tem uma exploração conhecida.
- Pacotes afetados: lista cada pacote identificado como vulnerável na descoberta e os detalhes de cada pacote:

- Filepath — O ID do volume do EBS e o número da partição associados a uma descoberta. Este campo está presente nas descobertas de instâncias do EC2 verificadas usando Verificação sem agente.
- Versão instalada/Versão fixa: o número da versão do pacote atualmente instalado para o qual uma vulnerabilidade foi detectada. Compare o número da versão instalada com o valor após a barra (/). O segundo valor é o número da versão do pacote que corrige a vulnerabilidade detectada, conforme fornecido pelas CVEs (vulnerabilidades e exposições comuns) ou pelo aviso associado à descoberta. Se a vulnerabilidade tiver sido corrigida em várias versões, esse campo listará a versão mais recente que inclui a correção. Se uma correção não estiver disponível, esse valor será `None available`.

  > **Note**
  >
  > Se uma descoberta foi detectada antes que o Amazon Inspector começasse a incluir esse campo nas descobertas, o valor desse campo estará vazio. No entanto, uma correção pode estar disponível.

- Gerenciador de pacotes: o gerenciador de pacotes usado para configurar esse pacote.
- Correção: se uma correção estiver disponível por meio de um pacote atualizado ou biblioteca de programação, esta seção incluirá os comandos que você poderá executar para fazer a atualização. Copie o comando fornecido e execute-o em seu ambiente.

  > **Note**
  >
  > Os comandos de correção são fornecidos pelos feeds de dados do fornecedor e podem variar dependendo da configuração do sistema. Consulte as referências de descoberta ou a documentação do sistema operacional para obter orientações mais específicas.

- Detalhes da vulnerabilidade: fornece um link para a fonte preferencial do Amazon Inspector para a CVE identificada na descoberta, como o NVD (Banco de dados nacional de vulnerabilidades), REDHAT ou outro fornecedor de sistema operacional. Além disso, você encontrará as pontuações de gravidade da descoberta. Para obter mais informações sobre a pontuação de gravidade, como, consulte Níveis de severidade para descobertas do Amazon Inspector. As seguintes pontuações estão incluídas, inclusive os vetores de pontuação de cada uma:
  - Pontuação do EPSS
  - Pontuação do Inspector

- CVSS 3.1 da CVE do Amazon
- CVSS 3.1 de NVD
- CVSS 2.0 do NVD (quando aplicável, para as CVEs mais antigas)

- Vulnerabilidades relacionadas: especifica outras vulnerabilidades relacionadas à descoberta. Normalmente, esses são outras CVEs que afetam a mesma versão do pacote ou outras CVEs dentro do mesmo grupo da CVE de descoberta, conforme determinado pelo fornecedor.

Vulnerabilidade de código

As descobertas de vulnerabilidade de código estão disponíveis somente para funções do Lambda. Consulte Vulnerabilidade de código para obter mais informações. Esse tipo de descoberta tem os seguintes detalhes:

- Correção disponível: para vulnerabilidades de código, esse valor é sempre `YES`.
- Nome do detector — O nome do CodeGuru detector usado para detectar a vulnerabilidade do código. Para obter uma lista de possíveis detecções, consulte a Biblioteca de CodeGuru Detectores.
- Etiquetas do detector — As CodeGuru etiquetas associadas ao detector CodeGuru usam etiquetas para categorizar as detecções.
- CWE relevantes: IDs das Enumerações Comuns de Fraqueza CWE (associadas à vulnerabilidade do código).
- Caminho do arquivo: o local do arquivo da vulnerabilidade do código.
- Local da vulnerabilidade: para vulnerabilidades de código de escaneamento de código do Lambda, esse campo mostra as linhas exatas de código em que o Amazon Inspector encontrou a vulnerabilidade.
- Correção sugerida: isso sugere como o código pode ser editado para corrigir a descoberta.

Acessibilidade de rede

As descobertas de acessibilidade da rede estão disponíveis apenas para instâncias do EC2. Consulte Acessibilidade de rede para obter mais informações. Esse tipo de descoberta tem os seguintes detalhes:

- Intervalo de portas abertas: o intervalo de portas por meio do qual a instância do EC2 pode ser acessada.
- Caminhos de rede abertos: mostra o caminho de acesso aberto para a instância do EC2. Selecione um item no caminho para obter mais informações.
- Correção: recomenda um método para fechar o caminho de rede aberto.

# Pontuação do Amazon Inspector e inteligência de vulnerabilidade

No console do Amazon Inspector, ao selecionar uma descoberta, você pode visualizar a guia Pontuação do Inspector e a inteligência de vulnerabilidade, que mostra os detalhes da pontuação de uma descoberta de vulnerabilidade do pacote, bem como detalhes da inteligência de vulnerabilidade. Esses detalhes estão disponíveis apenas para descobertas Vulnerabilidade do pacote.

## Pontuação do Amazon Inspector

A pontuação do Amazon Inspector é uma pontuação contextualizada que o Amazon Inspector cria para cada descoberta de instância do EC2. A pontuação do Amazon Inspector é determinada pela correlação das informações básicas de pontuação do CVSS v3.1 com as informações coletadas do seu ambiente de computação durante as verificações, como resultados de acessibilidade da rede e dados de explorabilidade. Por exemplo, a pontuação do Amazon Inspector de uma descoberta pode ser menor do que a pontuação base se a vulnerabilidade for explorável pela rede, mas o Amazon Inspector determina que nenhum caminho de rede aberto para a instância vulnerável está disponível na internet.

A pontuação base para uma descoberta é a pontuação base do CVSS v3.1 fornecida pelo fornecedor. As pontuações básicas de fornecedores do RHEL, Debian ou Amazon têm suporte, para outros fornecedores, ou casos em que o fornecedor não forneceu uma pontuação. O Amazon Inspector usa a pontuação base do NVD (Banco de dados nacional de vulnerabilidades). O Amazon Inspector usa a Calculadora do Common Vulnerability Scoring System Versão 3.1 para calcular a pontuação. Você pode ver a origem da pontuação básica de uma descoberta individual nos detalhes da descoberta, em detalhes da vulnerabilidade, como Fonte de vulnerabilidade (ou packageVulnerabilityDetails.source no JSON da descoberta)

> **Note**
>
> A pontuação do Amazon Inspector não está disponível para instâncias do Linux executando o Ubuntu. Isso ocorre porque o Ubuntu define a própria gravidade de vulnerabilidade, que pode diferir da gravidade da CVE associada.

### Detalhes de pontuação do Amazon Inspector

Ao abrir a página de detalhes de uma descoberta, você pode selecionar a guia Pontuação do Inspector e a inteligência de vulnerabilidade. Esse painel mostra a diferença entre a pontuação base

e a pontuação do Inspector. Esta seção explica como o Amazon Inspector atribuiu a classificação de severidade com base em uma combinação da pontuação do Amazon Inspector e da pontuação do fornecedor para o pacote de software. Se as pontuações forem diferentes, este painel mostra uma explicação do porquê.

Na seção de Métricas de pontuação CVSS, você pode ver uma tabela com comparações entre as métricas de pontuação base do CVSS e a pontuação do Inspector. As métricas comparadas são as métricas básicas definidas no documento de especificação do CVSS mantido pela first.org. A seguir é apresentado um resumo das métricas básicas:

Vetor de ataque

O contexto pelo qual uma vulnerabilidade pode ser explorada. No caso de descobertas do Amazon Inspector, isso pode ser Rede, Rede Adjacente ou Local.

Complexidade do ataque

Isso descreve o nível de dificuldade que um invasor enfrentará ao explorar a vulnerabilidade. Uma pontuação Baixa significa que o atacante precisará atender a pouca ou nenhuma condição adicional para explorar a vulnerabilidade. Uma pontuação Alta significa que um invasor precisará investir uma quantidade considerável de esforço para realizar um ataque bem-sucedido com essa vulnerabilidade.

Privilégios Obrigatórios

Isso descreve o nível de privilégio que um invasor precisará para explorar uma vulnerabilidade.

Interação com o usuário

Essa métrica indica se um ataque bem-sucedido usando essa vulnerabilidade requer um usuário humano, que não seja o atacante.

Scope

Isso indica se uma vulnerabilidade em um componente vulnerável afeta os recursos em componentes além do escopo de segurança do componente vulnerável. Se esse valor for Inalterado, o recurso afetado e o recurso impactado serão iguais. Se esse valor for Alterado, o componente vulnerável poderá ser explorado para impactar os recursos gerenciados por diferentes autoridades de segurança.

Confidencialidade

Isso mede o nível de impacto na confidencialidade dos dados em um recurso quando a vulnerabilidade é explorada. Isso varia de Nenhuma, onde nenhuma confidencialidade é perdida,

até Alta, onde todas as informações dentro de um recurso são divulgadas ou informações confidenciais, como senhas ou chaves de criptografia, podem ser divulgadas.

Integridade

Isso mede o nível de impacto na integridade dos dados dentro do recurso afetado se a vulnerabilidade for explorada. A integridade está em risco quando o invasor modifica arquivos dentro dos recursos afetados. A pontuação varia de Nenhuma, em que a exploração não permite que um invasor modifique nenhuma informação, até Alta, em que, se explorada, a vulnerabilidade permitiria que um invasor modificasse qualquer um ou todos os arquivos, ou os arquivos que poderiam ser modificados teriam consequências graves.

Disponibilidade

Isso mede o nível de impacto na disponibilidade do recurso afetado quando a vulnerabilidade é explorada. A pontuação varia de Nenhuma, quando a vulnerabilidade não afeta a disponibilidade, até Alta, em que, se explorada, o invasor pode negar completamente a disponibilidade do recurso ou fazer com que um serviço fique indisponível.

## Inteligência de vulnerabilidade

Esta seção resume a inteligência disponível sobre a CVE da Amazon, bem como as fontes de inteligência de segurança padrão do setor, como Futuro Registrado e CISA (Agência de Segurança Cibernética e de Infraestrutura).

> **Note**
>
> Intel da CISA, Amazon ou Recorded Future não estarão disponíveis para todas as CVEs.

Você pode ver os detalhes da inteligência de vulnerabilidade no console ou usando a API BatchGetFindingDetails. Os detalhes a seguir estão disponíveis no console:

ATT&CK

Esta seção mostra as TTPs (táticas, técnicas e procedimentos) do MITRE associados à CVE. As TTPs associados são mostrados. Se houver mais de duas TTPs aplicáveis, você poderá selecionar o link para visualizar uma lista completa. Selecionar uma tática ou técnica abre informações sobre ela no site do MITRE.

CISA

Esta seção aborda as datas relevantes associadas à vulnerabilidade. A data em que a CISA (Agência de Segurança Cibernética e de Infraestrutura) adicionou a vulnerabilidade ao Catálogo de Vulnerabilidades Exploradas Conhecidas, com base em evidências de exploração ativa, e a data de vencimento que a CISA espera que os sistemas sejam corrigidos. Essas informações são provenientes da CISA.

Malware conhecido

Esta seção mostra ferramentas e kits de exploração conhecidos que exploram essa vulnerabilidade.

Evidências

Esta seção resume os eventos de segurança mais críticos envolvendo essa vulnerabilidade. Se mais de 3 eventos tiverem o mesmo nível de caráter crítico, os três principais eventos mais recentes serão exibidos.

Hora do último relatório

Esta seção mostra a data da última exploração pública conhecida dessa vulnerabilidade.

# Níveis de severidade para descobertas do Amazon Inspector

Quando o Amazon Inspector gera uma descoberta de vulnerabilidade, ele atribui automaticamente uma severidade à descoberta. A gravidade de uma descoberta reflete as principais respectivas características e, portanto, pode ajudar você a avaliar e priorizar suas descobertas. A gravidade de uma descoberta não implica nem indica o caráter crítico ou a importância que um recurso afetado pode ter para sua organização.

A classificação de severidade de uma descoberta é determinada por uma pontuação numérica que corresponde a um dos seguintes níveis de severidade: informativo, baixo, médio, alto ou crítico.

O método pelo qual o Amazon Inspector determina a gravidade difere de acordo com o tipo de descoberta. Consulte as seções a seguir para saber mais sobre como o Amazon Inspector determina a classificação de severidade para cada tipo de descoberta.

## Gravidade da vulnerabilidade do pacote de software

O Amazon Inspector usa a pontuação do NVD/CVSS como base da pontuação de severidade para vulnerabilidades de pacotes de software. A pontuação do NVD/CVSS é a pontuação de

gravidade da vulnerabilidade publicada pelo NVD e definida pelo CVSS. A pontuação do NVD/CVSS é uma composição de métricas de segurança, como complexidade do ataque, maturidade do código de exploração e privilégios necessários. O Amazon Inspector produz uma pontuação numérica de 1 a 10 que reflete a gravidade da vulnerabilidade. O Amazon Inspector classifica isso como uma pontuação básica porque reflete a gravidade de uma vulnerabilidade de acordo com suas características intrínsecas, que são constantes ao longo do tempo. Essa pontuação também pressupõe o pior impacto razoável em diferentes ambientes implantados. O padrão CVSS v3 mapeia as pontuações do CVSS para as seguintes classificações de gravidade.

| Pontuação | Classificação |
|---|---|
| 0 | Informativo |
| 0,1—3,9 | Baixo |
| 4,0—6,9 | Médio |
| 7,0—8,9 | Alta |
| 9,0—10,0 | Crítico |

As descobertas de vulnerabilidade do pacote também podem ter uma severidade de Não triado. Isso significa que o fornecedor ainda não definiu uma pontuação de vulnerabilidade para a vulnerabilidade detectada. Nesse caso, é recomendável usar os URLs de referência para a descoberta para pesquisar essa vulnerabilidade e responder adequadamente.

As descobertas de vulnerabilidade do pacote incluem as seguintes pontuações e os vetores de pontuação associados como parte dos detalhes da descoberta:

- Pontuação do EPSS
- Pontuação do Inspector
- CVSS 3.1 da CVE do Amazon
- CVSS 3.1 de NVD
- CVSS 2.0 do NVD (quando aplicável)

## Gravidade da vulnerabilidade do código

Para descobertas de vulnerabilidade de código, o Amazon Inspector usa os níveis de severidade definidos pelos CodeGuru detectores da Amazon que geraram a descoberta. Cada detector recebe uma severidade usando o sistema de pontuação do CVSS v3. Para obter uma explicação sobre os CodeGuru usos de severidade, consulte Definições de severidade no CodeGuru guia. Para obter uma lista de detectores por gravidade, selecione uma das linguagens de programação compatíveis abaixo:

- Detectores Python por gravidade
- Detectores Java por gravidade

## Gravidade da acessibilidade da rede

O Amazon Inspector determina a gravidade de uma vulnerabilidade de acessibilidade da rede com base no serviço, nas portas e nos protocolos expostos e pelo tipo de caminho aberto. A tabela a seguir define essas classificações de severidade. O valor na coluna Open Path Rating representa caminhos abertos de gateways virtuais, VPCs com peering e redes. AWS Direct Connect Todos os outros serviços, portas e protocolos expostos têm uma classificação de severidade informativa.

| Serviço | Portas TCP | Portas UDP | Classificação do caminho da Internet | Classificação do caminho aberto |
|---|---|---|---|---|
| DHCP | 67, 68, 546, 547 | 67, 68, 546, 547 | Médio | Informativo |
| Elasticsearch | 9300, 9200 | N/D | Médio | Informativo |
| FTP | 21 | 21 | Alta | Médio |
| LDAP de catálogo global | 3268 | N/D | Médio | Informativo |
| LDAP de catálogo global sobre TLS | 3269 | N/D | Médio | Informativo |
| HTTP | 80 | 80 | Baixo | Informativo |

| | | | | |
|---|---|---|---|---|
| HTTPS | 443 | 443 | Baixo | Informativo |
| Kerberos | 88, 464, 543, 544, 749, 751 | 88, 464, 749, 750, 751, 752 | Médio | Informativo |
| LDAP | 389 | 389 | Médio | Informativo |
| LDAP por TLS | 636 | N/D | Médio | Informativo |
| MongoDB | 27017, 27018, 27019, 28017 | N/D | Médio | Informativo |
| MySQL | 3306 | N/D | Médio | Informativo |
| NetBIOS | 137, 139 | 137, 138 | Médio | Informativo |
| NFS | 111, 2049, 4045, 1110 | 111, 2049, 4045, 1110 | Médio | Informativo |
| Oracle | 1521, 1630 | N/D | Médio | Informativo |
| PostgreSQL | 5432 | N/D | Médio | Informativo |
| Serviços de impressão | 515 | N/D | Alta | Médio |
| RDP | 3389 | 3389 | Médio | Baixo |
| RPC | 111, 135, 530 | 111, 135, 530 | Médio | Informativo |
| SMB | 445 | 445 | Médio | Informativo |
| SSH | 22 | 22 | Médio | Baixo |
| SQL Server | 1433 | 1434 | Médio | Informativo |
| Syslog | 601 | 514 | Médio | Informativo |
| Telnet | 23 | 23 | Alta | Médio |
| WINS | 1512, 42 | 1512, 42 | Médio | Informativo |

# Gerenciar descobertas no Amazon Inspector

O Amazon Inspector oferece várias maneiras de classificar, agrupar e gerenciar suas descobertas. Esses recursos ajudam você a adaptar as descobertas ao seu ambiente, agregar descobertas por meio de diferentes visualizações e focar nas vulnerabilidades do seu ambiente específico. AWS

As descobertas aparecem em várias visualizações com base em seu estado: ativo, suprimido ou fechado. Por padrão, cada visualização mostra somente descobertas ativas. Uma descoberta ativa representa um possível problema de segurança detectado pelo Amazon Inspector que indica uma vulnerabilidade ou ameaça potencial. As descobertas suprimidas são descobertas ativas que você excluiu usando regras de supressão. O Amazon Inspector define automaticamente o status de uma descoberta como fechada quando detecta que a descoberta foi corrigida. Você não fecha manualmente as descobertas.

Você também pode ver as descobertas em AWS Security Hub, um serviço que fornece uma visão abrangente do seu estado de segurança em todo o seu AWS ambiente. Para ter mais informações, consulte Integração do Amazon Inspector com AWS Security Hub. As descobertas de imagens de contêineres também estão disponíveis no console do Amazon ECR, e você pode visualizar as descobertas de todos os recursos usando o AWS Command Line Interface (AWS CLI) ou a API.

Tópicos



## Visualizar as descobertas do Amazon Inspector

O console do Amazon Inspector exibe as descobertas em visualizações tabuladas com base em agrupamentos relacionados. Cada visualização inclui informações que podem ajudá-lo a analisar vulnerabilidades específicas, identificar seus recursos mais vulneráveis e avaliar o impacto geral das vulnerabilidades em seu ambiente. Navegue para uma visualização de descoberta diferente escolhendo uma opção no painel lateral de navegação de Descobertas. Também é possível criar

um filtro em cada exibição para se concentrar em tipos específicos de descobertas. Para obter mais informações sobre o uso de filtros, consulte Filtrar as descobertas do Amazon Inspector.

As descobertas podem ser agrupadas pelos seguintes parâmetros:

- Por vulnerabilidade: lista as vulnerabilidades mais críticas detectadas em seu ambiente. Escolha um título de vulnerabilidade nessa exibição para abrir um painel de detalhes com informações adicionais.
- Por conta: lista suas contas, a porcentagem de cobertura de verificação do Amazon Inspector, para cada conta e o número total de descobertas de severidade crítica e alta para cada conta. Esse agrupamento está disponível somente para administradores delegados.
- Por instância: lista as instâncias do Amazon EC2 mais vulneráveis no seu ambiente.
- Por imagem de contêiner: lista as imagens de contêiner do Amazon ECR mais vulneráveis em seu ambiente.
- Por repositório de contêineres: mostra os repositórios com mais vulnerabilidades.
- Por função do Lambda: mostra as funções do Lambda com mais vulnerabilidades.
- Todas as descobertas: mostra uma lista completa das descobertas do seu ambiente. Essa é a visualização padrão ao navegar até a página Descobertas. Nessa exibição, filtre por descobertas ativas, suprimidas e fechadas.

Crie regras de supressão com base em filtros para excluir descobertas das visualizações de descobertas. Para ter mais informações, consulte Suprimir descobertas do Amazon Inspector com regras de supressão.

# Filtrar as descobertas do Amazon Inspector

Um filtro de descoberta permite visualizar somente as descobertas que correspondem aos critérios especificados. As descobertas que não correspondem aos critérios do filtro são excluídas da sua visualização. Crie filtros de descobertas no console do Amazon Inspector. Para usar esses filtros para suprimir automaticamente descobertas existentes e futuras, consulte Suprimir descobertas do Amazon Inspector com regras de supressão.

## Criar filtros no console do Amazon Inspector

Em cada visualização de descobertas, use a funcionalidade de filtro para localizar descobertas com características específicas. Os filtros são removidos ao se mover para uma exibição com guias diferente.

Um filtro é composto por um critério de filtro, que consiste em um atributo de filtro emparelhado com um valor de filtro. As descobertas que não correspondem aos seus critérios de filtro são excluídas da lista de descobertas. Por exemplo, para ver todas as descobertas associadas à sua conta de administrador, você pode escolher o atributo ID da AWS conta e combiná-lo com o valor da ID da AWS conta de doze dígitos.

Alguns critérios de filtro se aplicam a todas as descobertas, enquanto outros estão disponíveis para tipos de recursos específicos ou somente para tipos de descoberta.

Para aplicar um filtro à visualização de descobertas

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. No painel de navegação, selecione Descobertas. A visualização padrão exibe todas as descobertas com um status Ativo.
3. Para filtrar as descobertas por critérios, selecione a barra Adicionar filtro para consultar uma lista de todos os critérios de filtro aplicáveis a essa exibição. Diferentes critérios de filtro estão disponíveis em diferentes visualizações.
4. Escolha um critério a ser filtrado na lista.
5. No painel de entrada de critérios, insira os valores de filtro desejados para definir esse critério.
6. Escolha Aplicar para aplicar esse critério de filtro aos seus resultados atuais. É possível continuar adicionando outro critério de filtro selecionando a barra de entrada do filtro novamente.
7. (Opcional) Para visualizar suas descobertas suprimidas ou fechadas, escolha Ativo na barra de filtro e, em seguida, escolha Suprimido ou Fechado. Escolha Mostrar tudo para visualizar descobertas ativas, suprimidas e fechadas na mesma exibição.

# Suprimir descobertas do Amazon Inspector com regras de supressão

Use regras de supressão para excluir descobertas que correspondam aos critérios. Por exemplo, você pode criar uma regra que suprima todas as descobertas com pontuações baixas de vulnerabilidade, para que você possa se concentrar somente nas descobertas mais críticas.

> **Note**
>
> As regras de supressão são usadas somente para filtrar sua lista de descobertas e não têm nenhum impacto nas descobertas nem impedem que o Amazon Inspector gere descobertas.

Se o Amazon Inspector gerar descobertas que correspondam a uma regra de supressão, as descobertas serão definidas como Suprimidas. As descobertas que correspondem a uma regra de supressão não aparecem na sua lista por padrão.

O Amazon Inspector armazena descobertas suprimidas até que sejam corrigidas. O Amazon Inspector detecta descobertas corrigidas. Quando o Amazon Inspector detecta uma descoberta corrigida, ele define a descoberta como Fechada e a armazena por 7 dias.

As descobertas suprimidas são publicadas na Amazon AWS Security Hub e EventBridge como eventos. Você pode suprimir automaticamente descobertas indesejadas no Security Hub alterando o status das descobertas usando uma EventBridge regra. Para obter mais informações, consulte Como criar regras de supressão automática em. AWS Security Hub

Você não pode criar uma regra de supressão que feche ou corrija as descobertas. Você só pode criar uma regra de supressão para filtrar quais descobertas aparecem na sua lista. Visualize as descobertas suprimidas a qualquer momento no console do Amazon Inspector.

> **Note**
>
> As contas dos membros em uma organização não podem criar nem gerenciar regras de supressão.

## Criar uma regra de supressão

Crie regras de supressão para filtrar a lista de descobertas que são mostradas por padrão. Você pode criar uma regra de supressão programaticamente usando a CreateFilterAPI e especificando `SUPRESS` como valor para. `action`

> **Note**
>
> Somente contas independentes e administradores delegados do Amazon Inspector podem criar e gerenciar regras de supressão. Os membros de uma organização não verão uma opção para regras de supressão no painel de navegação.

Para criar uma regra de supressão (console)

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. No painel de navegação, escolha Regras de supressão. Em seguida, escolha Create rule (Criar regra).
3. Para cada critério, faça o seguinte:
   - Selecione a barra de filtro para visualizar uma lista de critérios de filtro que você poderá adicionar à sua regra de supressão.
   - Selecione os critérios de filtro para sua regra de supressão.
4. Quando terminar de adicionar os critérios, insira um nome para a regra e uma descrição opcional.
5. Selecione a apção Salvar regra. O Amazon Inspector aplica imediatamente a nova regra de supressão e oculta todas as descobertas que correspondam aos critérios.

## Visualizar as descobertas suprimidas

Por padrão, o Amazon Inspector não exibe descobertas suprimidas no console do Amazon Inspector. No entanto, você poderá ver as descobertas suprimidas por uma regra específica.

Para visualizar descobertas suprimidas

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. No painel de navegação, selecione Regras de supressão.
3. Na lista de regras de supressão, selecione o título da regra.

## Alterar as regras de supressão

É possível fazer alterações nas funções de supressão a qualquer momento.

Para modificar as regras de supressão

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home
2. No painel de navegação, selecione Regras de supressão.
3. Selecione o título da regra de supressão a ser modificada.
4. Faça as alterações pretendidas e escolha Salvar para atualizar a regra.

## Excluir regras de supressão

Exclua as funções de supressão. Se excluir uma regra de supressão, o Amazon Inspector interrompe a supressão de ocorrências novas e existentes de descobertas que atendam aos critérios da regra e que não sejam suprimidas por outras regras.

Depois de excluir uma regra de supressão, ocorrências novas e existentes de descobertas que atendam aos critérios da regra têm o status Ativo. Isso significa que eles aparecem por padrão no console do Amazon Inspector. Além disso, o Amazon Inspector publica essas descobertas no AWS Security Hub e na Amazon EventBridge como eventos.

Para excluir uma regra de supressão

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. No painel de navegação, selecione Regras de supressão.
3. Marque a caixa de seleção ao lado do título da regra de supressão do que deseja excluir.
4. Escolha Excluir e, em seguida, confirme sua escolha de excluir permanentemente a regra.

# Exportação de relatórios de descobertas do Amazon Inspector

Além de enviar descobertas para a Amazon EventBridge AWS Security Hub, você pode, opcionalmente, exportá-las para um bucket do Amazon Simple Storage Service (Amazon S3) como um relatório de descobertas. Um relatório de descobertas é um arquivo CSV ou JSON que contém os detalhes das descobertas que você escolhe incluir no relatório. Ele fornece um resumo detalhado das descobertas em um momento específico. Para cada descoberta, o arquivo inclui detalhes como o nome do recurso da Amazon (ARN) do recurso afetado, a data e a hora em que a descoberta foi criada, o ID do Common Vulnerabilities and Exposures (CVE) associado e a gravidade, o status e as pontuações do Amazon Inspector e do CVSS da descoberta.

Ao configurar um relatório de descobertas, você começa especificando quais descobertas incluir no relatório. Por padrão, o Amazon Inspector inclui dados de todas as descobertas atuais do Região da AWS que têm o status de Ativo. Se você for o administrador delegado do Amazon Inspector para uma organização, isso inclui dados de descobertas para todas as contas membros em sua organização.

Opcionalmente, você pode personalizar um relatório filtrando os dados. Com filtros, inclua ou exclua dados de descobertas que tenham características específicas como, por exemplo, todas as descobertas críticas criadas durante um intervalo de tempo específico, todas as descobertas ativas de um recurso específico ou todas as descobertas críticas de um tipo específico. Se você for o administrador do Amazon Inspector de uma organização, você pode usar filtros para criar um relatório que inclua descobertas de um item específico Conta da AWS em sua organização — por exemplo, todas as descobertas críticas de uma conta que tenham um status de Ativo e para as quais uma correção esteja disponível. Em seguida, você pode compartilhar o relatório com o proprietário da conta para remediação.

> **Note**
>
> Ao exportar um relatório de descobertas usando a CreateFindingsReportAPI, você só verá as descobertas ativas por padrão. Para ver descobertas suprimidas ou fechadas, você deve especificar `SUPPRESSED` ou `CLOSED` como valores para os critérios do filtro findingStatus.

Quando você exporta um relatório de descobertas, o Amazon Inspector criptografa os dados com uma chave AWS Key Management Service (AWS KMS) que você especifica e adiciona o relatório a um bucket do S3 que você também especifica. A chave de criptografia deve ser uma chave de criptografia simétrica AWS Key Management Service (AWS KMS) gerenciada pelo cliente que esteja na atual Região da AWS. Além disso, a política de chaves deve permitir que o Amazon Inspector use a chave. O bucket do S3 também deve estar na região atual, e a política do bucket deve permitir que o Amazon Inspector adicione objetos ao bucket.

Depois que o Amazon Inspector terminar de criptografar e armazenar o relatório, você pode baixar o relatório do bucket do S3 especificado ou movê-lo para outro local. Como alternativa, você pode manter o relatório no mesmo bucket do S3 e usar esse bucket como um repositório para relatórios de descobertas que podem ser exportados posteriormente.

Este tópico orienta você pelo processo de uso do AWS Management Console para exportar um relatório de descobertas. O processo consiste em verificar se você tem as permissões necessárias, configurar os recursos necessários e, em seguida, configurar e exportar o relatório.

> **Note**
>
> Você pode exportar somente um relatório de descobertas por vez. Se uma exportação estiver em andamento, aguarde até que seja concluída antes de tentar exportar dados adicionais.

Tarefas

- Etapa 1: verificar as permissões
- Etapa 2: configurar um bucket do Amazon S3
- Etapa 3: configurar o AWS KMS key
- Etapa 4: configurar e exportar um relatório de descobertas
- Solucionar erros de exportação

Depois de exportar um relatório de descobertas pela primeira vez, as etapas 1 a 3 podem ser opcionais. Isso depende principalmente se você deseja usar o mesmo bucket do S3 e AWS KMS key para relatórios subsequentes.

Se você preferir exportar um relatório programaticamente após as etapas 1 a 3, use a CreateFindingsReportoperação da API do Amazon Inspector.

## Etapa 1: verificar as permissões

Antes de exportar um relatório de descobertas do Amazon Inspector, verifique se você tem as permissões necessárias para exportar relatórios de descobertas e configurar recursos para criptografar e armazenar os relatórios. Para verificar suas permissões, use AWS Identity and Access Management (IAM) para revisar as políticas do IAM que estão anexadas à sua identidade do IAM. Em seguida, compare as informações nessas políticas com a seguinte lista de ações que você deve ter permissão para realizar para exportar o relatório de descobertas.

Amazon Inspector

Para o Amazon Inspector, verifique se você tem permissão para realizar as seguintes ações:

- `inspector2:ListFindings`

- `inspector2:CreateFindingsReport`

Essas ações permitem que você recupere dados de descobertas para sua conta e exporte esses dados em relatórios de descobertas.

Se você planeja exportar relatórios grandes programaticamente, você também pode verificar se tem permissão para realizar as seguintes ações: `inspector2:GetFindingsReportStatus` para verificar o status dos relatórios e `inspector2:CancelFindingsReport` cancelar as exportações que estão em andamento.

AWS KMS

Para AWS KMS, verifique se você tem permissão para realizar as seguintes ações:

- `kms:GetKeyPolicy`
- `kms:PutKeyPolicy`

Essas ações permitem que você recupere e atualize a política de chaves para o AWS KMS key que você deseja que o Amazon Inspector use para criptografar seu relatório.

Para usar o console do Amazon Inspector para exportar um relatório, verifique também se você tem permissão para realizar as seguintes AWS KMS ações:

- `kms:DescribeKey`
- `kms:ListAliases`

Essas ações permitem que você recupere e exiba informações sobre o AWS KMS keys para sua conta. Em seguida, você pode escolher uma dessas chaves para criptografar o relatório.

Se você planeja criar uma nova chave KMS para criptografar o relatório, você também precisa ter permissão para realizar a ação do `kms:CreateKey`.

Amazon S3

Para o Amazon S3, verifique se você tem permissão para realizar as seguintes ações:

- `s3:CreateBucket`
- `s3:DeleteObject`
- `s3:PutBucketAcl`
- `s3:PutBucketPolicy`
- `s3:PutBucketPublicAccessBlock`
- `s3:PutObject`

- `s3:PutObjectAcl`

  Essas ações permitem criar e configurar o bucket do S3 no qual você deseja que o Amazon Inspector armazene o relatório. Elas também permitem que você adicione e exclua objetos do bucket.

  Para usar o console do Amazon Inspector para exportar um relatório, verifique também se você tem permissão para realizar as seguintes ações do `s3:ListAllMyBuckets` e `s3:GetBucketLocation`: Essas ações permitem que você recupere e exiba informações sobre os buckets do S3 para sua conta. Em seguida, você pode escolher um desses buckets para armazenar o relatório.

Se você não tiver permissão para realizar uma ou mais das ações necessárias, peça ajuda ao administrador do AWS antes de prosseguir para a próxima etapa.

## Etapa 2: configurar um bucket do Amazon S3

Depois de verificar as permissões, você estará pronto para configurar o bucket do S3 no qual deseja armazenar o relatório de descobertas. Pode ser um bucket existente para sua própria conta ou um bucket existente de propriedade de outra pessoa Conta da AWS e que você tem permissão para acessar. Se você quiser armazenar o relatório em um novo bucket, crie o bucket antes de continuar.

O bucket do S3 deve estar nos Região da AWS mesmos dados das descobertas que você deseja exportar. Por exemplo, se você estiver usando o Amazon Inspector na região Leste dos EUA (Norte da Virgínia) e quiser exportar dados de descobertas para essa região, o bucket também deverá estar na região Leste dos EUA (Norte da Virgínia).

Além disso, a política do bucket deve permitir que o Amazon Inspector adicione objetos ao bucket. Este tópico explica como atualizar a política de bucket e fornece um exemplo da declaração a ser adicionada à política. Para obter mais informações sobre buckets e políticas atualizadas, consulte Uso de políticas de bucket no Guia do usuário do Amazon Simple Storage Service.

Se você quiser armazenar o relatório em um bucket do S3 que pertence a outra conta, trabalhe com o proprietário do bucket para atualizar a política do bucket. Obtenha também o URI do bucket. Você precisará fornecer esse URI ao exportar o relatório.

Para atualizar a política de bucket:

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3.

2. No painel de navegação, escolha Buckets.
3. Escolha o bucket do S3 no qual você deseja armazenar o relatório de descobertas.
4. Escolha a aba Permissions.
5. Na seção Bucket policy, selecione Edit.
6. Copie o seguinte exemplo de declaração para a área de transferência:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "allow-inspector",
   "Effect": "Allow",
   "Principal": {
    "Service": "inspector2.amazonaws.com"
   },
   "Action": [
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:AbortMultipartUpload"
   ],
   "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
   "Condition": {
    "StringEquals": {
     "aws:SourceAccount": "111122223333"
    },
    "ArnLike": {
     "aws:SourceArn": "arn:aws:inspector2:Region:111122223333:report/*"
    }
   }
  }
 ]
}
```

7. No editor de políticas do Bucket no console do Amazon S3, cole a declaração anterior na política para adicioná-la à política.

   Ao adicionar a instrução, verifique se a sintaxe é válida. As políticas de bucket usam o formato JSON. Isso significa que você precisa adicionar uma vírgula antes ou depois da declaração, dependendo de onde você adiciona a declaração à política. Se você incluir a instrução como a última instrução, adicione uma vírgula após o colchete de fechamento para a instrução anterior.

Se você adicioná-la como a primeira instrução ou adicioná-la entre duas instruções existentes, adicione uma vírgula após o colchete de fechamento.

8. Atualize a instrução com os valores corretos para seu ambiente, onde:

   - *DOC-EXAMPLE-BUCKET é o nome do bucket*.
   - *111122223333* é o ID da conta para o Conta da AWS.
   - A *região* é aquela Região da AWS em que você está usando o Amazon Inspector e deseja permitir que o Amazon Inspector adicione relatórios ao bucket. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`.

   > **Note**
   >
   > Se você estiver usando o Amazon Inspector de forma ativada manualmente Região da AWS, adicione também o código de região apropriado ao valor do campo. `Service` Esse campo especifica o responsável pelo serviço do Amazon Inspector.
   > Por exemplo, se você estiver usando o Amazon Inspector na região do Oriente Médio (Bahrein), que tem o código da região `me-south-1`, substitua `inspector2.amazonaws.com` por `inspector2.me-south-1.amazonaws.com` na instrução.

   A instrução de exemplo define as condições que usam duas chaves de condição globais do IAM:

   - aws: SourceAccount — Essa condição permite que o Amazon Inspector adicione relatórios ao bucket somente para sua conta. Isso impede que o Amazon Inspector adicione relatórios ao bucket para outras contas. Mais especificamente, a condição especifica qual conta pode usar o bucket para os recursos e ações especificados pela condição do `aws:SourceArn`.

     Para armazenar relatórios de contas adicionais no bucket, adicione o ID da conta de cada conta adicional a essa condição. Por exemplo: .

     ```
     "aws:SourceAccount": [111122223333,444455556666,123456789012]
     ```

   - aws: SourceArn — Essa condição restringe o acesso ao bucket com base na origem dos objetos que estão sendo adicionados ao bucket. Isso impede que outros Serviços da AWS adicionem objetos ao bucket. Também impede que o Amazon Inspector adicione objetos ao bucket enquanto executa outras ações na sua conta. Mais especificamente, a condição

permite que o Amazon Inspector adicione objetos ao bucket somente se os objetos forem relatórios de descobertas e somente se esses relatórios forem criados pela conta e na região especificada na condição.

Para permitir que o Amazon Inspector execute as ações especificadas para contas adicionais, adicione os nomes do recurso da Amazon (ARNs) para cada conta adicional a essa condição. Por exemplo: .

```
"aws:SourceArn": [
    "arn:aws:inspector2:Region:111122223333:report/*",
    "arn:aws:inspector2:Region:444455556666:report/*",
    "arn:aws:inspector2:Region:123456789012:report/*"
]
```

As contas especificadas pelas condições `aws:SourceAccount` e `aws:SourceArn` devem ser correspondentes.

As duas condições ajudam a evitar que o Amazon Inspector seja usado como um representante confuso durante transações com o Amazon S3. Embora não seja recomendável, você pode remover essas condições da política de bucket.

9. Quando terminar de atualizar a política do bucket, escolha Salvar alterações.

## Etapa 3: configurar o AWS KMS key

Depois de verificar as permissões e configurar o bucket do S3, determine qual AWS KMS key você deseja que o Amazon Inspector use para criptografar o relatório de descobertas. A chave deve ser uma chave do KMS de criptografia simétrica e gerenciada pelo cliente. Além disso, a chave deve estar no mesmo Região da AWS bucket do S3 que você configurou para armazenar o relatório.

A chave pode ser uma chave KMS existente da sua conta ou uma chave KMS existente de outra pessoa. Se você planeja usar uma nova chave para as descobertas do KMS, crie uma chave antes de prosseguir. Se quiser usar uma chave existente de outra conta, obtenha o nome do recurso da Amazon (ARN) da chave. Você precisará fornecer esse URI ao exportar o relatório do Amazon Inspector. Para obter informações sobre como criar e revisar as configurações das chaves KMS, consulte Gerenciamento de chaves no Guia do desenvolvedor do AWS Key Management Service .

Depois de determinar qual chave do KMS você deseja usar, dê permissão ao Amazon Inspector para usar a chave. Caso contrário, o Amazon Inspector não poderá criptografar e exportar o relatório.

Para dar permissão ao Amazon Inspector para usar a chave, atualize a política de chaves para a chave. Para obter informações detalhadas sobre políticas de chaves e gerenciamento do acesso às chaves do KMS, consulte Políticas de chaves no AWS KMS no Guia do desenvolvedor do AWS Key Management Service .

Atualizar a política de chaves

> **Note**
>
> O procedimento a seguir é para atualizar uma chave existente para permitir que o Amazon Inspector a use. Se você ainda não tiver uma chave existente, consulte https://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html para obter orientação sobre como criar uma.

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. No painel de navegação, escolha Chaves gerenciadas pelo cliente.
4. Escolha a chave do KMS que você deseja usar para criptografar o relatório. A chave deve ser de criptografia simétrica (SYMMETRIC_DEFAULT).
5. Na guia Política de chave, escolha Editar. Se você não ver uma política de chave com um botão Editar, primeiro selecione Alternar para a exibição de política.
6. Copie o seguinte exemplo de declaração para a área de transferência:

```
{
    "Sid": "Allow Amazon Inspector to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": "inspector2.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        },
```

```
        "ArnLike": {
            "aws:SourceArn": "arn:aws:inspector2:Region:111122223333:report/*"
        }
    }
}
```

7. No editor de políticas de chaves no AWS KMS console, cole a declaração anterior na política de chaves para adicioná-la à política.

   Ao adicionar a instrução, verifique se a sintaxe é válida. As políticas de chave usam o formato JSON. Isso significa que você precisa adicionar uma vírgula antes ou depois da declaração, dependendo de onde você adiciona a declaração à política. Se você incluir a instrução como a última instrução, adicione uma vírgula após o colchete de fechamento para a instrução anterior. Se você adicioná-la como a primeira instrução ou adicioná-la entre duas instruções existentes, adicione uma vírgula após o colchete de fechamento.

8. Atualize a instrução com os valores corretos para seu ambiente, onde:

   - *111122223333* é o ID da conta para o Conta da AWS.
   - A *região* é a Região da AWS na qual você deseja permitir que o Amazon Inspector criptografe relatórios com a chave. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`.

   > **Note**
   >
   > Se você estiver usando o Amazon Inspector de forma ativada manualmente Região da AWS, adicione também o código de região apropriado ao valor do campo. `Service` Por exemplo, se você estiver usando o Amazon Inspector na região Oriente Médio (Bahrein), substitua `inspector2.amazonaws.com` por `inspector2.me-south-1.amazonaws.com`.

   Assim como a declaração de exemplo da política de bucket na etapa anterior, os campos da `Condition` neste exemplo usam duas chaves de condição globais do IAM:

   - aws: SourceAccount — Essa condição permite que o Amazon Inspector execute as ações especificadas somente para sua conta. Mais especificamente, determina qual conta pode executar as ações especificadas para os recursos e ações especificadas pelo `aws:SourceArn`.

Para permitir que o Amazon Inspector execute as ações especificadas para contas adicionais, adicione o ID da conta de cada conta adicional a esta condição. Por exemplo: .

```
"aws:SourceAccount": [111122223333,444455556666,123456789012]
```

- aws: SourceArn — Essa condição impede que outras pessoas Serviços da AWS executem as ações especificadas. Ela também impede que o Amazon Inspector use a chave enquanto executa outras ações na sua conta. Em outras palavras, ela permite que o Amazon Inspector criptografe objetos do S3 com a chave somente se os objetos forem relatórios de descobertas e somente se esses relatórios forem criados pela conta e na região especificada na condição.

  Para permitir que o Amazon Inspector execute as ações especificadas para contas adicionais, adicione os nomes do recurso da Amazon para cada conta adicional a essa condição. Por exemplo: .

```
"aws:SourceArn": [
    "arn:aws:inspector2:us-east-1:111122223333:report/*",
    "arn:aws:inspector2:us-east-1:444455556666:report/*",
    "arn:aws:inspector2:us-east-1:123456789012:report/*"
]
```

  As contas especificadas pelas condições `aws:SourceAccount` e `aws:SourceArn` devem ser correspondentes.

Essas condições ajudam a evitar que o Amazon Inspector seja usado como um representante confuso durante transações com. AWS KMS Embora não seja recomendável, você pode remover essas condições da instrução.

9. Quando terminar de atualizar a política de chave, escolha Salvar alterações.

## Etapa 4: configurar e exportar um relatório de descobertas

Depois de verificar suas permissões e configurar os recursos para criptografar e armazenar o relatório de descobertas, você estará pronto para configurar e exportar o relatório.

Para configurar e exportar um relatório de descobertas

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.

2. No painel de navegação, em Descobertas, selecione Todas as descobertas.
3. (Opcional) Usando a barra de filtro acima da tabela Descobertas, adicione critérios de filtro que especifiquem quais descobertas incluir no relatório. Conforme você adiciona critérios, o Amazon Inspector atualiza a tabela para incluir somente as descobertas que correspondem aos critérios. A tabela fornece uma visualização prévia dos dados que o relatório conterá.

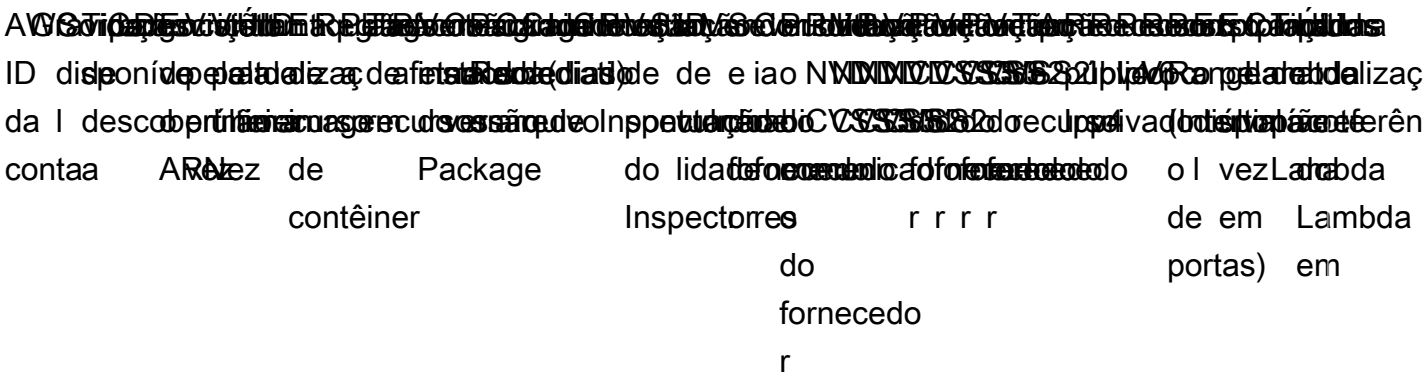
   > **Note**
   >
   > Recomendamos que você adicione critérios de filtro. Caso contrário, o relatório incluirá dados de todas as suas descobertas atuais Região da AWS que tenham um status de Ativo. Se você for o administrador do Amazon Inspector para uma organização, isso inclui dados de descobertas para todas as contas membros em sua organização.
   > Se um relatório incluir dados de todas ou muitas descobertas, pode levar muito tempo para gerar e exportar o relatório, e você poderá exportar somente um relatório por vez.

4. Escolha Exportar descobertas.
5. Na seção Configurações de exportação, em Tipo de arquivo de exportação, especifique um formato de arquivo para o relatório:

   - Para criar um arquivo de notação de JavaScript objeto (.json) que contém os dados, escolha JSON.

     Se você escolher a opção JSON, o relatório incluirá todos os campos de cada descoberta. Para obter uma lista de possíveis campos JSON, consulte o tipo de dados Descoberta na referência da API do Amazon Inspector.
   - Para criar um arquivo de valores separados por vírgula (.csv) que contenha os dados, escolha CSV.

     Se você escolher a opção CSV, o relatório incluirá somente um subconjunto dos campos para cada descoberta, aproximadamente 45 campos que relatam os principais atributos de uma descoberta. Os campos incluem: tipo de descoberta, título, gravidade, status, descrição, vista pela primeira vez, vista pela última vez, correção disponível, ID da conta da AWS , ID do recurso, tags de recursos e Correção. Eles são um acréscimo aos campos que capturam detalhes de pontuação e URLs de referência para cada descoberta. Veja a seguir uma amostra dos cabeçalhos CSV em um relatório de descobertas:



6. Em Local de exportação, para URI do S3, especifique o bucket do S3 em que você deseja armazenar o relatório:

   - Para armazenar o relatório em um bucket de propriedade da conta, escolha Browse S3. O Amazon Inspector exibe uma tabela dos buckets do S3 para a conta. Escolha o bucket que deseja usar e, em seguida, escolha Escolher.

     > **Tip**
     >
     > Para especificar também um prefixo de caminho do Amazon S3 para o relatório, acrescente uma barra (/) e o prefixo ao valor na caixa URI do S3. O Amazon Inspector então inclui o prefixo quando adiciona o relatório ao bucket, e o Amazon S3 gera o caminho especificado pelo prefixo.
     > Por exemplo, se você quiser usar seu Conta da AWS ID como prefixo e o ID da sua conta for 111122223333, acrescente o valor na caixa URI do **/111122223333** S3.
     > Um prefixo é semelhante a um caminho de diretório em um bucket do S3. Ele permite agrupar objetos semelhantes em um bucket, da mesma forma que você pode armazenar arquivos semelhantes em uma pasta em um sistema de arquivos. Para obter informações sobre como usar pastas no Amazon S3, consulte Usar pastas no Manual do usuário do console do Amazon Simple Storage Service.

   - Para armazenar o relatório em um bucket de propriedade de outra conta, insira o URI do bucket como, por exemplo, **s3://DOC-EXAMPLE_BUCKET**, em que DOC-EXAMPLE_BUCKET é o nome do bucket. O proprietário do bucket pode encontrar essas informações para você nas propriedades do bucket.

7. Para a chave KMS, especifique a AWS KMS key que você deseja usar para criptografar o relatório:

- Para usar uma chave da sua conta, escolha a chave na lista. A lista exibe chaves KMS de criptografia simétrica e gerenciadas pelo cliente para sua conta.
- Se quiser usar uma chave existente de outra conta, obtenha o nome do recurso da Amazon (ARN) da chave. O proprietário da chave pode encontrar essas informações para você nas propriedades da chave. Para obter informações, consulte Encontrar o ID da chave e o ARN no Guia do desenvolvedor do AWS Key Management Service .

8. Escolha Exportar.

O Amazon Inspector gera o relatório de descobertas, criptografa-o com a chave KMS que você especificou e o adiciona ao bucket S3 que você especificou. Dependendo do número de descobertas que você optou por incluir no relatório, esse processo pode levar vários minutos ou horas. Quando a exportação estiver concluída, o Amazon Inspector exibirá uma mensagem indicando que seu relatório de descobertas foi exportado com sucesso. Opcionalmente, escolha Visualizar relatório na mensagem para navegar até o relatório no Amazon S3.

Você pode exportar somente um relatório de descobertas por vez. Se uma exportação estiver em andamento, aguarde até que seja concluída antes de tentar exportar dados adicionais.

## Solucionar erros de exportação

Se ocorrer um erro ao tentar exportar um relatório de descobertas, o Amazon Inspector exibirá uma mensagem descrevendo o erro. Use as informações neste tópico como um guia para identificar possíveis causas e soluções para o erro.

Por exemplo, verifique se o bucket do S3 está no atual Região da AWS e se a política do bucket permite que o Amazon Inspector adicione objetos ao bucket. Verifique também se o AWS KMS key está habilitado na região atual e garanta que a política de chaves permita que o Amazon Inspector use a chave.

Depois de solucionar o erro, tente exportar o relatório novamente.

### Não é possível ter vários relatórios de erro

Se você estiver tentando criar um relatório, mas o Amazon Inspector já estiver gerando um relatório, você receberá um erro informando Motivo: Não é possível ter vários relatórios em andamento. Esse erro ocorre porque o Amazon Inspector só pode gerar um relatório para uma conta por vez.

Para resolver o erro, você pode esperar que o outro relatório seja concluído ou cancelá-lo antes de solicitar um novo relatório.

Você pode verificar o status de um relatório usando a GetFindingsReportStatusoperação. Essa operação retorna o ID do relatório de qualquer relatório que esteja sendo gerado no momento.

Se necessário, você pode usar o ID do relatório fornecido pela `GetFindingsReportStatus` operação para cancelar uma exportação que está em andamento usando a CancelFindingsReportoperação.

# Criação de respostas personalizadas às descobertas do Amazon Inspector com a Amazon EventBridge

O Amazon Inspector cria um evento para a Amazon EventBridge para descobertas recém-geradas, descobertas recém-agregadas e mudanças no estado das descobertas. Qualquer coisa que não seja uma alteração nos campos `updatedAt` e `lastObservedAt` publicará um novo evento. Isso significa que novos eventos para uma descoberta são gerados ao realizar ações como reiniciar um recurso ou alterar as tags associadas a um recurso. No entanto, o ID de descoberta no campo `id` permanece o mesmo. Os eventos são emitidos com base no melhor esforço.

> **Note**
>
> Se sua conta for um administrador delegado do Amazon Inspector, EventBridge publica eventos em sua conta, além da conta de membro da qual eles se originaram.

Ao usar EventBridge eventos com o Amazon Inspector, você pode automatizar tarefas para ajudá-lo a responder aos problemas de segurança revelados pelas descobertas do Amazon Inspector.

O Amazon Inspector emite eventos para o barramento de eventos padrão na mesma região. Isso significa que você deverá configurar regras de eventos para cada região na qual você está executando o Amazon Inspector para visualizar os eventos dessa região.

Para receber notificações sobre descobertas do Amazon Inspector com base em EventBridge eventos, você deve criar uma EventBridge regra e uma meta para o Amazon Inspector. Essa regra permite EventBridge enviar notificações de descobertas que o Amazon Inspector gera para o alvo especificado na regra. Para obter mais informações, consulte EventBridgeas regras da Amazon no Guia EventBridge do usuário da Amazon.

# Esquema de eventos

Este é um exemplo do formato de eventos do Amazon Inspector para um evento de descoberta do EC2. Por exemplo, esquema de outros tipos de descoberta e tipos de eventos, consulte EventBridge esquema.


```
{
    "version": "0",
    "id": "66a7a279-5f92-971c-6d3e-c92da0950992",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T22:46:15Z",
    "region": "us-east-1",
    "resources": ["i-0c2a343f1948d5205"],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "\n It was discovered that the sound subsystem in the Linux
 kernel contained a\n race condition in some situations. A local attacker could use
 this to cause\n a denial of service (system crash).",
        "exploitAvailable": "YES",
        "exploitabilityDetails": {
            "lastKnownExploitAt": "Oct 24, 2022, 11:08:59 PM"
        },
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "fixAvailable": "YES",
        "lastObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "packageVulnerabilityDetails": {
            "cvss": [{
                "baseScore": 4.7,
                "scoringVector": "CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H",
                "source": "NVD",
                "version": "3.1"
            }],
            "referenceUrls": ["https://lore.kernel.org/all/
CAFcO6XN7JDM4xSXGhtusQfS2mSBcx50VJKwQpCq=WeLt57aaZA@mail.gmail.com/", "https://
ubuntu.com/security/notices/USN-5792-1", "https://ubuntu.com/security/notices/
USN-5791-2", "https://ubuntu.com/security/notices/USN-5791-1", "https://ubuntu.com/
security/notices/USN-5793-2", "https://git.kernel.org/pub/scm/linux/kernel/git/
torvalds/linux.git/commit/?id=8423f0b6d513b259fdab9c9bf4aaa6188d054c2d", "https://
ubuntu.com/security/notices/USN-5793-1", "https://ubuntu.com/security/notices/
```

```
USN-5792-2", "https://ubuntu.com/security/notices/USN-5791-3", "https://ubuntu.com/
security/notices/USN-5793-4", "https://ubuntu.com/security/notices/USN-5793-3",
 "https://git.kernel.org/linus/8423f0b6d513b259fdab9c9bf4aaa6188d054c2d(6.0-rc5)",
 "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3303"],
            "relatedVulnerabilities": [],
            "source": "UBUNTU_CVE",
            "sourceUrl": "https://people.canonical.com/~ubuntu-security/cve/2022/
CVE-2022-3303.html",
            "vendorCreatedAt": "Sep 27, 2022, 11:15:00 PM",
            "vendorSeverity": "medium",
            "vulnerabilityId": "CVE-2022-3303",
            "vulnerablePackages": [{
                "arch": "X86_64",
                "epoch": 0,
                "fixedInVersion": "0:5.15.0.1027.31~20.04.16",
                "name": "linux-image-aws",
                "packageManager": "OS",
                "remediation": "apt update && apt install --only-upgrade linux-image-
aws",
                "version": "5.15.0.1026.30~20.04.16"
            }]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [{
            "details": {
                "awsEc2Instance": {
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b7ff1a8d69f1bb35",
                    "ipV4Addresses": ["172.31.85.212", "44.203.45.27"],
                    "ipV6Addresses": [],
                    "launchedAt": "Jan 19, 2023, 7:53:14 PM",
                    "platform": "UBUNTU_20_04",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
            "id": "i-0c2a343f1948d5205",
            "partition": "aws",
```

```
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "CVE-2022-3303 - linux-image-aws",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 10:46:15 PM"
    }
}
```


# Criação de uma EventBridge regra para notificá-lo das descobertas do Amazon Inspector

Para aumentar a visibilidade das descobertas do Amazon Inspector, você pode usar EventBridge para configurar alertas de busca automatizados que são enviados para um hub de mensagens. Este tópico mostra como enviar alertas para `CRITICAL` e descobertas de gravidade `HIGH` para e-mail, Slack ou Amazon Chime. Você aprenderá como configurar um tópico do Amazon Simple Notification Service e depois conectar esse tópico a uma regra de EventBridge evento.

## Etapa 1. Configurar um tópico e um endpoint do Amazon SNS

Para configurar alertas automáticos, primeiro configure um tópico no Amazon Simple Notification Service e adicione um endpoint. Para obter mais informações, consulte o Guia do SNS.

Este procedimento estabelece para a qual você deseja enviar dados de descobertas do Amazon Inspector. O tópico do SNS pode ser adicionado a uma regra de EventBridge evento durante ou após a criação da regra de evento.

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. No painel de navegação, selecione Tópicos e selecione Criar Tópico.
3. Na seção Criar tópico, selecione Padrão. Em seguida, insira um nome de tópico, como **`Inspector_to_Email`**. Os outros detalhes são opcionais.
4. Selecione Criar tópico. Isso abre um novo painel com detalhes do seu novo tópico.
5. Na seção Assinatura, escolha Criar assinatura.

6. a. No menu Protocolo selecione E-mail.
   b. No campo Endpoint, insira 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 após a criação da assinatura.

   c. Selecione Criar assinatura.
7. Procure 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. No painel de navegação, selecione Tópicos e selecione Criar Tópico.
3. Na seção Criar tópico, selecione Padrão. Em seguida, insira um nome de tópico, como **`Inspector_to_Slack`**. Os outros detalhes são opcionais. Escolha Criar tópico para concluir a criação do endpoint.

Configurando um cliente AWS Chatbot

1. Navegue até o AWS Chatbot console emhttps://console.aws.amazon.com/chatbot/.
2. No painel Clientes configurados, selecione Configurar novo cliente.
3. Selecione Slack e, em seguida, selecione Configurar para confirmar.

> **Note**
>
> Ao escolher o Slack, confirme as permissões de AWS Chatbot para 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.

c. No Slack, copie o ID do canal privado clicando com o botão direito do mouse no nome do canal e selecionando Link de cópia.

d. Em AWS Management Console, na AWS Chatbot janela, cole o ID do canal que você copiou do Slack no campo ID do canal privado.

e. Em Permissões, escolha criar um perfil do IAM usando um modelo se você ainda não tiver uma função.

f. Em Modelos de política, selecione Permissões de notificação. Esse é o modelo de política do IAM para AWS Chatbot. Essa política fornece as permissões necessárias de leitura e lista para CloudWatch alarmes, eventos e registros e para tópicos do Amazon SNS.

g. Para políticas de proteção do canal, escolha AmazonInspector 2. ReadOnlyAccess

h. Escolha 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.

### Amazon 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 seguida, insira um nome de tópico, como **`Inspector_to_Chime`**. Os outros detalhes são opcionais. Escolha Criar tópico para concluir.

#### Configurando um cliente AWS Chatbot

1. Navegue até o AWS Chatbot console emhttps://console.aws.amazon.com/chatbot/.
2. No painel Clientes configurados, selecione Configurar novo cliente.
3. Selecione Chime e, em seguida, escolha Configurar para confirmar.
4. No painel Detalhes da configuração, insira um nome para o canal.
5. No Amazon Chime, abra a sala de chat 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. Em AWS Management Console, na AWS Chatbot janela, cole o URL que você copiou no campo URL do webhook.
7. Em Permissões, escolha criar um perfil do IAM usando um modelo se você ainda não tiver uma função.
8. Em Modelos de política, selecione 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. Escolha 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 Amazon Chime.
10. Selecione Configurar.

## Etapa 2. Crie uma EventBridge regra para as descobertas do Amazon Inspector

1. Abra o EventBridge console da Amazon em https://console.aws.amazon.com/events/.
2. Selecione Regras no painel de navegação e selecione Criar regra.
3. Insira um nome e uma descrição opcional para a regra.
4. Selecione Regra com um padrão de evento e depois Avançar.
5. No painel Padrão de Evento, escolha Padrões personalizados (editor JSON).
6. Cole o JSON a seguir no editor.

```
{
  "source": ["aws.inspector2"],
  "detail-type": ["Inspector2 Finding"],
  "detail": {
    "severity": ["HIGH", "CRITICAL"],
    "status": ["ACTIVE"]
  }
}
```

> **Note**
>
> Esse padrão envia notificações para qualquer descoberta ativa `CRITICAL` ou de gravidade `HIGH` detectada pelo Amazon Inspector.

Selecione Avançar quando terminar de inserir o padrão do evento.

7. Na página Selecionar destinos, escolha AWS service (Serviço da AWS). Em seguida, em Selecionar tipo de destino, escolha o tópico SNS.
8. Em Tópico selecione o nome do tópico do SNS criado na Etapa 1. Em seguida, escolha Próximo.
9. Adicione tags opcionais, se necessário, e escolha Avançar.
10. Verifique sua regra e selecione Criar regra.

## EventBridge para ambientes de várias contas do Amazon Inspector

Se você for um administrador delegado do Amazon Inspector, EventBridge as regras aparecerão em sua conta com base nas descobertas aplicáveis de suas contas de membros. Se você configurar notificações de descobertas EventBridge em sua conta de administrador, conforme detalhado na seção anterior, você receberá notificações sobre várias contas. Em outras palavras, você será notificado sobre descobertas e eventos gerados por suas contas de membros, além daqueles gerados por sua própria conta.

Use os detalhes da `accountId` do JSON da descoberta para identificar a conta membro da qual a descoberta do Amazon Inspector se originou.

# Exportação de SBOMs com o Amazon Inspector

Use o console ou a API do Amazon Inspector para gerar uma lista de materiais de software (SBOM) para seus recursos. Um SBOM é um inventário aninhado de todos os componentes de software de código aberto e de terceiros da sua base de código. O Amazon Inspector fornece SBOMs para recursos individuais no seu ambiente. Os SBOMs exportados do Amazon Inspector podem ajudar você para obter visibilidade das informações sobre seu fornecimento de software, como os pacotes mais usados e as vulnerabilidades associadas em toda a sua organização.

Exporte os SBOMs para todos os recursos compatíveis monitorados ativamente pelo Amazon Inspector. Revise o status de seus recursos em Avaliar a cobertura do Amazon Inspector sobre seu ambiente da AWS.

> **Note**
>
> O Amazon Inspector não suporta a exportação de SBOM para instâncias do Windows EC2.

## Formatos do Amazon Inspector

O Amazon Inspector suporta a exportação de SBOMs nos formatos compatíveis com CycloneDX 1.4 e SPDX 2.3. O Amazon Inspector exporta os SBOMs como arquivos do `JSON` ao bucket do Amazon S3 que você escolher.

> **Note**
>
> As exportações no formato SPDX do Amazon Inspector são compatíveis com sistemas que usam o SPDX 2.3, no entanto, elas não contêm o campo CC0 (Creative Commons Zero). Isso ocorre porque a inclusão desse campo permitiria que os usuários redistribuíssem ou editassem o material.

### Exemplo do formato CycloneDX 1.4 SBOM do Amazon Inspector

```
                {
"bomFormat": "CycloneDX",
"specVersion": "1.4",
```

```
  "version": 1,
  "metadata": {
    "timestamp": "2023-06-02T01:17:46Z",
    "component": null,
    "properties": [
      {
        "name": "imageId",
        "value":
 "sha256:c8ee97f7052776ef223080741f61fcdf6a3a9107810ea9649f904aa4269fdac6"
      },
      {
        "name": "architecture",
        "value": "arm64"
      },
      {
        "name": "accountId",
        "value": "111122223333"
      },
      {
        "name": "resourceType",
        "value": "AWS_ECR_CONTAINER_IMAGE"
      }
    ]
  },
  "components": [
    {
      "type": "library",
      "name": "pip",
      "purl": "pkg:pypi/pip@22.0.4?path=usr/local/lib/python3.8/site-packages/
pip-22.0.4.dist-info/METADATA",
      "bom-ref": "98dc550d1e9a0b24161daaa0d535c699"
    },
    {
      "type": "application",
      "name": "libss2",
      "purl": "pkg:dpkg/libss2@1.44.5-1+deb10u3?
arch=ARM64&epoch=0&upstream=libss2-1.44.5-1+deb10u3.src.dpkg",
      "bom-ref": "2f4d199d4ef9e2ae639b4f8d04a813a2"
    },
    {
      "type": "application",
      "name": "liblz4-1",
      "purl": "pkg:dpkg/liblz4-1@1.8.3-1+deb10u1?
arch=ARM64&epoch=0&upstream=liblz4-1-1.8.3-1+deb10u1.src.dpkg",
```

```
      "bom-ref": "9a6be8907ead891b070e60f5a7b7aa9a"
    },
    {
      "type": "application",
      "name": "mawk",
      "purl": "pkg:dpkg/mawk@1.3.3-17+b3?
arch=ARM64&epoch=0&upstream=mawk-1.3.3-17+b3.src.dpkg",
      "bom-ref": "c2015852a729f97fde924e62a16f78a5"
    },
    {
      "type": "application",
      "name": "libgmp10",
      "purl": "pkg:dpkg/libgmp10@6.1.2+dfsg-4+deb10u1?
arch=ARM64&epoch=2&upstream=libgmp10-6.1.2+dfsg-4+deb10u1.src.dpkg",
      "bom-ref": "52907290f5beef00dff8da77901b1085"
    },
    {
      "type": "application",
      "name": "ncurses-bin",
      "purl": "pkg:dpkg/ncurses-bin@6.1+20181013-2+deb10u3?
arch=ARM64&epoch=0&upstream=ncurses-bin-6.1+20181013-2+deb10u3.src.dpkg",
      "bom-ref": "cd20cfb9ebeeadba3809764376f43bce"
    }
  ],
  "vulnerabilities": [
    {
      "id": "CVE-2022-40897",
      "affects": [
        {
          "ref": "a74a4862cc654a2520ec56da0c81cdb3"
        },
        {
          "ref": "0119eb286405d780dc437e7dbf2f9d9d"
        }
      ]
    }
  ]
}
```


## Exemplo do formato SPDX 2.3 SBOM do Amazon Inspector

```
{
 "name": "409870544328/EC2/i-022fba820db137c64/ami-074ea14c08effb2d8",
 "spdxVersion": "SPDX-2.3",
 "creationInfo": {
  "created": "2023-06-02T21:19:22Z",
  "creators": [
   "Organization: 409870544328",
   "Tool: Amazon Inspector SBOM Generator"
  ]
 },
 "documentNamespace": "EC2://i-022fba820db137c64/AMAZON_LINUX_2/null/x86_64",
 "comment": "",
 "packages": [{
   "name": "elfutils-libelf",
   "versionInfo": "0.176-2.amzn2",
   "downloadLocation": "NOASSERTION",
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
    "referenceCategory": "PACKAGE-MANAGER",
    "referenceType": "purl",
    "referenceLocator": "pkg:rpm/elfutils-libelf@0.176-2.amzn2?
arch=X86_64&epoch=0&upstream=elfutils-libelf-0.176-2.amzn2.src.rpm"
   }],
   "SPDXID": "SPDXRef-Package-rpm-elfutils-libelf-ddf56a513c0e76ab2ae3246d9a91c463"
  },
  {
   "name": "libcurl",
   "versionInfo": "7.79.1-1.amzn2.0.1",
   "downloadLocation": "NOASSERTION",
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
     "referenceCategory": "PACKAGE-MANAGER",
     "referenceType": "purl",
     "referenceLocator": "pkg:rpm/libcurl@7.79.1-1.amzn2.0.1?
arch=X86_64&epoch=0&upstream=libcurl-7.79.1-1.amzn2.0.1.src.rpm"
    },
    {
     "referenceCategory": "SECURITY",
     "referenceType": "vulnerability",
     "referenceLocator": "CVE-2022-32205"
    }
   ],
```

```
    "SPDXID": "SPDXRef-Package-rpm-libcurl-710fb33829bc5106559bcd380cddb7d5"
   },
   {
    "name": "hunspell-en-US",
    "versionInfo": "0.20121024-6.amzn2.0.1",
    "downloadLocation": "NOASSERTION",
    "sourceInfo": "/var/lib/rpm/Packages",
    "filesAnalyzed": false,
    "externalRefs": [{
     "referenceCategory": "PACKAGE-MANAGER",
     "referenceType": "purl",
     "referenceLocator": "pkg:rpm/hunspell-en-US@0.20121024-6.amzn2.0.1?
arch=NOARCH&epoch=0&upstream=hunspell-en-US-0.20121024-6.amzn2.0.1.src.rpm"
    }],
    "SPDXID": "SPDXRef-Package-rpm-hunspell-en-US-de19ae0883973d6cea5e7e079d544fe5"
   },
   {
    "name": "grub2-tools-minimal",
    "versionInfo": "2.06-2.amzn2.0.6",
    "downloadLocation": "NOASSERTION",
    "sourceInfo": "/var/lib/rpm/Packages",
    "filesAnalyzed": false,
    "externalRefs": [{
      "referenceCategory": "PACKAGE-MANAGER",
      "referenceType": "purl",
      "referenceLocator": "pkg:rpm/grub2-tools-minimal@2.06-2.amzn2.0.6?
arch=X86_64&epoch=1&upstream=grub2-tools-minimal-2.06-2.amzn2.0.6.src.rpm"
     },
     {
      "referenceCategory": "SECURITY",
      "referenceType": "vulnerability",
      "referenceLocator": "CVE-2021-3981"
     }
    ],
    "SPDXID": "SPDXRef-Package-rpm-grub2-tools-minimal-c56b7ea76e5a28ab8f232ef6d7564636"
   },
   {
    "name": "unixODBC-devel",
    "versionInfo": "2.3.1-14.amzn2",
    "downloadLocation": "NOASSERTION",
    "sourceInfo": "/var/lib/rpm/Packages",
    "filesAnalyzed": false,
    "externalRefs": [{
     "referenceCategory": "PACKAGE-MANAGER",
```

```
    "referenceType": "purl",
    "referenceLocator": "pkg:rpm/unixODBC-devel@2.3.1-14.amzn2?
arch=X86_64&epoch=0&upstream=unixODBC-devel-2.3.1-14.amzn2.src.rpm"
   }],
   "SPDXID": "SPDXRef-Package-rpm-unixODBC-devel-1bb35add92978df021a13fc9f81237d2"
  }
 ],
 "relationships": [{
   "spdxElementId": "SPDXRef-DOCUMENT",
   "relatedSpdxElement": "SPDXRef-Package-rpm-elfutils-libelf-
ddf56a513c0e76ab2ae3246d9a91c463",
   "relationshipType": "DESCRIBES"
  },
  {
   "spdxElementId": "SPDXRef-DOCUMENT",
   "relatedSpdxElement": "SPDXRef-Package-rpm-yajl-8476ce2db98b28cfab2b4484f84f1903",
   "relationshipType": "DESCRIBES"
  },
  {
   "spdxElementId": "SPDXRef-DOCUMENT",
   "relatedSpdxElement": "SPDXRef-Package-rpm-unixODBC-
devel-1bb35add92978df021a13fc9f81237d2",
   "relationshipType": "DESCRIBES"
  }
 ],
 "SPDXID": "SPDXRef-DOCUMENT"
}
```


# Filtros para SBOMs

Ao exportar os SBOMs, você poderá incluir filtros para criar relatórios para subconjuntos específicos de recursos. Se não fornecer um filtro, os SBOMs de todos os recursos ativos compatíveis serão exportados. E se você for um administrador delegado, isso também inclui recursos para todos os membros. Os seguintes filtros estão disponíveis:

- AccountID: esse filtro pode ser usado para exportar os SBOMs para quaisquer recursos associados a uma ID de conta específica.
- Tag de instância do EC2: esse filtro pode ser usado para exportar os SBOMs para instâncias do EC2 com tags específicas.

- Nome da função: esse filtro pode ser usado para exportar os SBOMs para funções do Lambda específicas.
- Tag de imagem: esse filtro pode ser usado para exportar SBOMs para imagens de contêineres com tags específicas.
- Tag de função do Lambda: esse filtro pode ser usado para exportar SBOMs para funções do Lambda com tags específicas.
- Tipo de recurso: esse filtro pode ser usado para filtrar o tipo de recurso: EC2/ECR/Lambda.
- ID do recurso: esse filtro pode ser usado para exportar um SBOM para um recurso específico.
- Nome do repositório: esse filtro pode ser usado para gerar os SBOMs para imagens de contêiner em repositórios específicos.

## Configurar e exportar os SBOMs

Para exportar SBOMs, você deve primeiro configurar um bucket do Amazon S3 e AWS KMS uma chave que o Amazon Inspector tenha permissão para usar. Use filtros para exportar os SBOMs para subconjuntos específicos de seus recursos. Para exportar SBOMs para várias contas em uma AWS organização, siga estas etapas enquanto estiver conectado como administrador delegado do Amazon Inspector.

Pré-requisitos

- Recursos compatíveis que estão sendo monitorados ativamente pelo Amazon Inspector.
- Um bucket do Amazon S3 configurado com uma política que permite ao Amazon Inspector adicionar objetos a. Para obter informações sobre como configurar a política, consulte Configurar permissões de exportação.
- Uma AWS KMS chave configurada com uma política que permite que o Amazon Inspector use para criptografar seus relatórios. Para obter informações sobre como configurar a política, consulte Configurar uma AWS KMS chave para exportação.

> **Note**
>
> Se você configurou anteriormente um bucket do Amazon S3 e uma AWS KMS chave para exportação de descobertas, você pode usar o mesmo bucket e chave para a exportação do SBOM.

Selecione o método de acesso preferido para exportar um SBOM.

Console

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região com os recursos para os quais você deseja exportar o SBOM.
3. No painel de navegação, escolha Exportação de SBOMs.
4. (Opcional) Na página Exportar os SBOMs, use o menu Adicionar filtro para selecionar um subconjunto de recursos para os quais criar relatórios. Se nenhum filtro for fornecido, o Amazon Inspector exportará relatórios para todos os recursos ativos. Se você for um administrador delegado, isso incluirá todos os recursos ativos em sua organização.
5. Em Configuração de exportação, selecione o formato que você deseja para o SBOM.
6. Insira um URI do Amazon S3 ou escolha Procurar no Amazon S3 para selecionar um local do Amazon S3 para armazenar o SBOM.
7. Insira uma chave AWS KMS  configurada para o Amazon Inspector usar para criptografar seus relatórios.

API

- Para exportar SBOMs para seus recursos de forma programática, use a CreateSbomExportoperação da API do Amazon Inspector.

  Em sua solicitação, use o parâmetro `reportFormat` para especificar o formato de saída do SBOM, escolha `CYCLONEDX_1_4` ou `SPDX_2_3`. O parâmetro `s3Destination` é obrigatório, e você deve especificar um bucket do S3 configurado com uma política que permita que o Amazon Inspector grave nele. Opcionalmente, use os parâmetros `resourceFilterCriteria` para limitar o escopo do relatório a recursos específicos.

AWS CLI

- Para exportar SBOMs para seus recursos usando o AWS Command Line Interface comando a seguir:

```
aws inspector2 create-sbom-export --report-format
FORMAT --s3-destination bucketName=DOC-EXAMPLE-
BUCKET1,keyPrefix=PREFIX,kmsKeyArn=arn:aws:kms:Region:111122223333:key/123
```

Na solicitação, substitua *FORMAT* pelo formato de sua preferência, CYCLONEDX_1_4 ou SPDX_2_3. Em seguida, substitua o *user input placeholders* do destino do S3 pelo nome do bucket S3 a ser exportado, o prefixo a ser usado para a saída no S3 e o ARN da chave KMS que você está usando para criptografar os relatórios.

# Pesquisa no banco de dados de vulnerabilidades do Amazon Inspector

Você pode pesquisar vulnerabilidades e exposições (CVEs) no banco de dados de vulnerabilidades do Amazon Inspector. O Amazon Inspector usa informações do banco de dados de vulnerabilidades para produzir detalhes relacionados a uma ID CVE. Você pode acessar esses detalhes em uma página de detalhes do CVE.

Este tópico descreve como pesquisar o banco de dados de vulnerabilidade do Amazon Inspector usando um ID CVE e interpretar a página de detalhes do CVE. Para obter informações sobre descobertas, consulteDetalhes da descoberta do Amazon Inspector.

> **Note**
>
> O Amazon Inspector rastreia e produz descobertas para outras vulnerabilidades de software no banco de dados. No entanto, o Amazon Inspector só oferece suporte a CVEs com plataformas listadas na seção Plataformas de detecção da página de detalhes do CVE. Atualmente, a pesquisa CVE não é compatívelMicrosoft Windows.

## Pesquisando no banco de dados de vulnerabilidades

Esta seção descreve como pesquisar o banco de dados de vulnerabilidades no console e com a API do Amazon Inspector.

> **Note**
>
> Você deve ativar o Amazon Inspector em seu banco de dados atual Região da AWS antes de poder pesquisar o banco de dados de vulnerabilidades.

Console

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/
2. No painel de navegação, escolha Pesquisa de banco de dados de vulnerabilidade.
3. Na barra de pesquisa, insira uma ID CVE e escolha Pesquisar.

API

Execute a SearchVulnerabilitiesAPI do Amazon Inspector e forneça um único ID CVE `filterCriteria` no seguinte formato:. `CVE-<year>-<ID>`

# Entendendo os detalhes do CVE

Esta seção descreve como interpretar a página de detalhes do CVE.

## Detalhes do CVE

A seção de detalhes do CVE inclui as seguintes informações:

- Descrição e ID do CVE
- Gravidade da CVE
- Pontuações do Common Vulnerability Scoring System (CVSS) e do Exploit Prediction Scoring System (EPSS)
- Plataformas de detecção

> **Note**
>
> Se esse campo estiver vazio, o Amazon Inspector não suporta a detecção do seu ID CVE.

- Enumeração de fraquezas comuns (CWE)
- Datas criadas e atualizadas pelo fornecedor

## Inteligência de vulnerabilidade

A seção de inteligência de vulnerabilidade fornece dados de inteligência de ameaças, como alvos de exploração e a data da última exploração pública conhecida.

Ele também fornece dados da Agência de Segurança Cibernética e de Infraestrutura (CISA), que incluem a ação de remediação, a data em que o CVE foi adicionado ao catálogo de Vulnerabilidades Exploradas Conhecidas e a data em que a CISA espera que as agências federais corrijam o CVE.

## Referências

A seção de referências fornece links para recursos para obter mais informações sobre o CVE.

# Esquema de EventBridge eventos da Amazon para eventos do Amazon Inspector

Para suportar a integração com outros aplicativos, serviços e sistemas, como sistemas de monitoramento ou gerenciamento de eventos, o Amazon Inspector publica automaticamente as descobertas na Amazon EventBridge como eventos. EventBridgeé um serviço de barramento de eventos sem servidor que fornece um fluxo de dados em tempo real de aplicativos e outros Serviços da AWS para alvos, como AWS Lambda funções, tópicos do Amazon Simple Notification Service e streams do Amazon Kinesis Data Streams. Para saber mais sobre EventBridge eventos EventBridge e eventos, consulte o Guia EventBridge do usuário da Amazon.

O Amazon Inspector publica eventos para descobertas, mudanças na cobertura de recursos e verificações iniciais de recursos individuais. Cada evento é um objeto JSON que está em conformidade com o EventBridge esquema dos eventos. AWS Como os dados são estruturados como um EventBridge evento, você pode monitorar, processar e agir com mais facilidade de acordo com as descobertas e os eventos suportados do Amazon Inspector usando outros aplicativos, serviços e ferramentas.

Tópicos



## Esquema EventBridge básico da Amazon para o Amazon Inspector

A seguir está um exemplo do esquema básico de um EventBridge evento para o Amazon Inspector. Os detalhes do evento variam de acordo com o tipo de evento.

```
{
    "version": "0",
    "id": "Event ID",
    "detail-type": "Inspector2 *event type*",
    "source": "aws.inspector2",
    "account": "Conta da AWS ID (string)",
    "time": "event timestamp (string)",
```

```
    "region": "Região da AWS (string)",
    "resources": [
        *IDs or ARNs of the resources involved in the event*
    ],
    "detail": {
        *Details of an Amazon Inspector event type*
    }
}
```

# Exemplo de esquema de evento de descoberta do Amazon Inspector

A seguir estão alguns exemplos do esquema de um EventBridge evento para as descobertas do Amazon Inspector. Os eventos de descobertas são criados quando o Amazon Inspector identifica uma vulnerabilidade de software ou um problema de rede em um de seus recursos. Para obter um guia sobre como criar notificações em resposta a esse tipo de evento, consulte Criação de respostas personalizadas às descobertas do Amazon Inspector com a Amazon EventBridge.

Os campos a seguir identificam um evento de descoberta:

- O campo `detail-type` está definido como `Inspector2 Finding`.
- O objeto `detail` descreve a descoberta.

Selecione entre as opções para consultar como encontrar esquemas de eventos para diferentes recursos e tipos de descoberta.

Amazon EC2 package vulnerability finding

```
{
    "version": "0",
    "id": "66a7a279-5f92-971c-6d3e-c92da0950992",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T22:46:15Z",
    "region": "us-east-1",
    "resources": ["i-0c2a343f1948d5205"],
    "detail": {
        "awsAccountId": "111122223333",
```

```
        "description": "\n It was discovered that the sound subsystem in the Linux
 kernel contained a\n race condition in some situations. A local attacker could use
 this to cause\n a denial of service (system crash).",
        "exploitAvailable": "YES",
        "exploitabilityDetails": {
            "lastKnownExploitAt": "Oct 24, 2022, 11:08:59 PM"
        },
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "fixAvailable": "YES",
        "lastObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "packageVulnerabilityDetails": {
            "cvss": [{
                "baseScore": 4.7,
                "scoringVector": "CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H",
                "source": "NVD",
                "version": "3.1"
            }],
            "referenceUrls": ["https://lore.kernel.org/all/
CAFcO6XN7JDM4xSXGhtusQfS2mSBcx50VJKwQpCq=WeLt57aaZA@mail.gmail.com/", "https://
ubuntu.com/security/notices/USN-5792-1", "https://ubuntu.com/security/notices/
USN-5791-2", "https://ubuntu.com/security/notices/USN-5791-1", "https://ubuntu.com/
security/notices/USN-5793-2", "https://git.kernel.org/pub/scm/linux/kernel/git/
torvalds/linux.git/commit/?id=8423f0b6d513b259fdab9c9bf4aaa6188d054c2d", "https://
ubuntu.com/security/notices/USN-5793-1", "https://ubuntu.com/security/notices/
USN-5792-2", "https://ubuntu.com/security/notices/USN-5791-3", "https://ubuntu.com/
security/notices/USN-5793-4", "https://ubuntu.com/security/notices/USN-5793-3",
 "https://git.kernel.org/linus/8423f0b6d513b259fdab9c9bf4aaa6188d054c2d(6.0-rc5)",
 "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3303"],
            "relatedVulnerabilities": [],
            "source": "UBUNTU_CVE",
            "sourceUrl": "https://people.canonical.com/~ubuntu-security/cve/2022/
CVE-2022-3303.html",
            "vendorCreatedAt": "Sep 27, 2022, 11:15:00 PM",
            "vendorSeverity": "medium",
            "vulnerabilityId": "CVE-2022-3303",
            "vulnerablePackages": [{
                "arch": "X86_64",
                "epoch": 0,
                "fixedInVersion": "0:5.15.0.1027.31~20.04.16",
                "name": "linux-image-aws",
                "packageManager": "OS",
```

```
                "remediation": "apt update && apt install --only-upgrade linux-
image-aws",
                "version": "5.15.0.1026.30~20.04.16"
            }]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [{
            "details": {
                "awsEc2Instance": {
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b7ff1a8d69f1bb35",
                    "ipV4Addresses": ["172.31.85.212", "44.203.45.27"],
                    "ipV6Addresses": [],
                    "launchedAt": "Jan 19, 2023, 7:53:14 PM",
                    "platform": "UBUNTU_20_04",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
            "id": "i-0c2a343f1948d5205",
            "partition": "aws",
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "CVE-2022-3303 - linux-image-aws",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 10:46:15 PM"
    }
}
```

## Amazon EC2 network reachability finding

```
{
```

```
    "version": "0",
    "id": "d0384f63-1621-1b75-d014-a5e45628ef3e",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T09:17:57Z",
    "region": "us-east-1",
    "resources": ["i-0a96278c2206a8e4b"],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "On the instance i-0a96278c2206a8e4b, the port range
 22-22 is reachable from the InternetGateway igw-72069c09 from an attached ENI
 eni-0976efe678170408f.",
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 20, 2023, 9:17:57 AM",
        "lastObservedAt": "Jan 20, 2023, 9:17:57 AM",
        "networkReachabilityDetails": {
            "networkPath": {
                "steps": [{
                    "componentId": "igw-72069c09",
                    "componentType": "AWS::EC2::InternetGateway"
                }, {
                    "componentId": "acl-91d74eec",
                    "componentType": "AWS::EC2::NetworkAcl"
                }, {
                    "componentId": "sg-0aaed0af450bd0165",
                    "componentType": "AWS::EC2::SecurityGroup"
                }, {
                    "componentId": "eni-0976efe678170408f",
                    "componentType": "AWS::EC2::NetworkInterface"
                }, {
                    "componentId": "i-0a96278c2206a8e4b",
                    "componentType": "AWS::EC2::Instance"
                }]
            },
            "openPortRange": {
                "begin": 22,
                "end": 22
            },
            "protocol": "TCP"
        },
        "remediation": {
            "recommendation": {
```

```
                "text": "You can restrict access to your instance by modifying the
 Security Groups or ACLs in the network path."
            }
        },
        "resources": [{
            "details": {
                "awsEc2Instance": {
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b5eea76982371e91",
                    "ipV4Addresses": ["3.89.90.19", "172.31.93.57"],
                    "ipV6Addresses": [],
                    "keyName": "example-inspector-test",
                    "launchedAt": "Jan 19, 2023, 7:25:02 PM",
                    "platform": "AMAZON_LINUX_2",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
            "id": "i-0a96278c2206a8e4b",
            "partition": "aws",
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "Port 22 is reachable from an Internet Gateway",
        "type": "NETWORK_REACHABILITY",
        "updatedAt": "Jan 20, 2023, 9:17:57 AM"
    }
}
```

## Amazon ECR package vulnerability finding

```
{
    "version": "0",
    "id": "5b52952e-26df-3a51-6d14-4dbe737e58ec",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
```

```
    "time": "2023-01-19T21:59:00Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ecr:us-east-1:111122223333:repository/inspector2/
sha256:98f0304b3a3b7c12ce641177a99d1f3be56f532473a528fda38d53d519cafb13"
    ],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "libcurl would reuse a previously created connection even
 when a TLS or SSHrelated option had been changed that should have prohibited
 reuse.libcurl keeps previously used connections in a connection pool for
 subsequenttransfers to reuse if one of them matches the setup. However, several TLS
 andSSH settings were left out from the configuration match checks, making themmatch
 too easily.",
        "exploitAvailable": "NO",
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 9:59:00 PM",
        "fixAvailable": "YES",
        "inspectorScore": 7.5,
        "inspectorScoreDetails": {
            "adjustedCvss": {
                "adjustments": [],
                "cvssSource": "NVD",
                "score": 7.5,
                "scoreSource": "NVD",
                "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N",
                "version": "3.1"
            }
        },
        "lastObservedAt": "Jan 19, 2023, 9:59:00 PM",
        "packageVulnerabilityDetails": {
            "cvss": [
                {
                    "baseScore": 5,
                    "scoringVector": "AV:N/AC:L/Au:N/C:N/I:P/A:N",
                    "source": "NVD",
                    "version": "2.0"
                },
                {
                    "baseScore": 7.5,
                    "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N",
                    "source": "NVD",
                    "version": "3.1"
```

```
                }
            ],
            "referenceUrls": [
                "https://hackerone.com/reports/1555796",
                "https://security.gentoo.org/glsa/202212-01",
                "https://lists.debian.org/debian-lts-announce/2022/08/
msg00017.html",
                "https://www.debian.org/security/2022/dsa-5197"
            ],
            "relatedVulnerabilities": [],
            "source": "NVD",
            "sourceUrl": "https://nvd.nist.gov/vuln/detail/CVE-2022-27782",
            "vendorCreatedAt": "Jun 2, 2022, 2:15:00 PM",
            "vendorSeverity": "HIGH",
            "vendorUpdatedAt": "Jan 5, 2023, 5:51:00 PM",
            "vulnerabilityId": "CVE-2022-27782",
            "vulnerablePackages": [
                {
                    "arch": "X86_64",
                    "epoch": 0,
                    "fixedInVersion": "0:7.61.1-22.el8_6.3",
                    "name": "libcurl",
                    "packageManager": "OS",
                    "release": "22.el8",
                    "remediation": "yum update libcurl",
                    "sourceLayerHash":
 "sha256:38a980f2cc8accf69c23deae6743d42a87eb34a54f02396f3fcfd7c2d06e2c5b",
                    "version": "7.61.1"
                },
                {
                    "arch": "X86_64",
                    "epoch": 0,
                    "fixedInVersion": "0:7.61.1-22.el8_6.3",
                    "name": "curl",
                    "packageManager": "OS",
                    "release": "22.el8",
                    "remediation": "yum update curl",
                    "sourceLayerHash":
 "sha256:38a980f2cc8accf69c23deae6743d42a87eb34a54f02396f3fcfd7c2d06e2c5b",
                    "version": "7.61.1"
                }
            ]
        },
        "remediation": {
```

```
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [
            {
                "details": {
                    "awsEcrContainerImage": {
                        "architecture": "amd64",
                        "imageHash":
 "sha256:98f0304b3a3b7c12ce641177a99d1f3be56f532473a528fda38d53d519cafb13",
                        "imageTags": [
                            "o3"
                        ],
                        "platform": "ORACLE_LINUX_8",
                        "pushedAt": "Jan 19, 2023, 7:38:39 PM",
                        "registry": "111122223333",
                        "repositoryName": "inspector2"
                    }
                },
                "id": "arn:aws:ecr:us-east-1:111122223333:repository/inspector2/
sha256:98f0304b3a3b7c12ce641177a99d1f3be56f532473a528fda38d53d519cafb13",
                "partition": "aws",
                "region": "us-east-1",
                "type": "AWS_ECR_CONTAINER_IMAGE"
            }
        ],
        "severity": "HIGH",
        "status": "ACTIVE",
        "title": "CVE-2022-27782 - libcurl, curl",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 9:59:00 PM"
    }
}
```

## Lambda package vulnerability finding

```
{
    "version": "0",
    "id": "040bb590-3a12-353f-ecb1-05e54b0fbea7",
    "detail-type": "Inspector2 Finding",
```

```
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T19:20:25Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:lambda:us-east-1:111122223333:function:ExampleFunction:$LATEST"
    ],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "Those using Woodstox to parse XML data may be vulnerable to
 Denial of Service attacks (DOS) if DTD support is enabled. If the parser is running
 on user supplied input, an attacker may supply content that causes the parser to
 crash by stackoverflow. This effect may support a denial of service attack.",
        "exploitAvailable": "NO",
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 7:20:25 PM",
        "fixAvailable": "YES",
        "inspectorScore": 7.5,
        "inspectorScoreDetails": {
            "adjustedCvss": {
                "cvssSource": "NVD",
                "score": 7.5,
                "scoreSource": "NVD",
                "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
                "version": "3.1"
            }
        },
        "lastObservedAt": "Jan 19, 2023, 7:20:25 PM",
        "packageVulnerabilityDetails": {
            "cvss": [
                {
                    "baseScore": 7.5,
                    "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
                    "source": "NVD",
                    "version": "3.1"
                }
            ],
            "referenceUrls": [
                "https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47434"
            ],
            "relatedVulnerabilities": [],
            "source": "NVD",
            "sourceUrl": "https://nvd.nist.gov/vuln/detail/CVE-2022-40152",
```

```
            "vendorCreatedAt": "Sep 16, 2022, 10:15:00 AM",
            "vendorSeverity": "HIGH",
            "vendorUpdatedAt": "Nov 25, 2022, 11:15:00 AM",
            "vulnerabilityId": "CVE-2022-40152",
            "vulnerablePackages": [
                {
                    "epoch": 0,
                    "filePath": "lib/woodstox-core-6.2.7.jar",
                    "fixedInVersion": "6.4.0",
                    "name": "com.fasterxml.woodstox:woodstox-core",
                    "packageManager": "JAR",
                    "remediation": "Update woodstox-core to 6.4.0",
                    "version": "6.2.7"
                }
            ]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [
            {
                "details": {
                    "awsLambdaFunction": {
                        "architectures": [
                            "X86_64"
                        ],
                        "codeSha256": "+EwrOrht2um4fdVCD73gj
+O7HJIAUvUxi8AD0eKHSkc=",
                        "executionRoleArn": "arn:aws:iam::111122223333:role/
ExampleFunction-ExecutionRole",
                        "functionName": "Example-function",
                        "lastModifiedAt": "Nov 7, 2022, 8:29:27 PM",
                        "packageType": "ZIP",
                        "runtime": "JAVA_11",
                        "version": "$LATEST"
                    }
                },
                "id": "arn:aws:lambda:us-
east-1:111122223333:function:ExampleFunction:$LATEST",
                "partition": "aws",
                "region": "us-east-1",
                "tags": {
```

```
                    "TargetAlias": "DeploymentStack",
                    "SoftwareType": "Infrastructure"
                },
                "type": "AWS_LAMBDA_FUNCTION"
            }
        ],
        "severity": "HIGH",
        "status": "ACTIVE",
        "title": "CVE-2022-40152 - com.fasterxml.woodstox:woodstox-core",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 7:20:25 PM"
    }
}
```

Lambda code vulnerability finding

```
{
   "version":"0",
   "id":"9df01cb1-df24-bc46-5650-085a4087e7aa",
   "detail-type":"Inspector2 Finding",
   "source":"aws.inspector2",
   "account":"111122223333",
   "time":"2023-12-07T22:14:45Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:lambda:us-east-1:111122223333:function:code-finding:$LATEST"
   ],
   "detail":{
      "awsAccountId":"111122223333",
      "codeVulnerabilityDetails":{
         "detectorId":"python/lambda-override-reserved@v1.0",
         "detectorName":"Override of reserved variable names in a Lambda function",
         "detectorTags":[
            "availability",
            "aws-python-sdk",
            "aws-lambda",
            "data-integrity",
            "maintainability",
            "security",
            "security-context",
            "python"
```

```
         ],
         "filePath":{
            "endLine":6,
            "fileName":"lambda_function.py",
            "filePath":"lambda_function.py",
            "startLine":6
         },
         "ruleId":"Rule-434311"
      },
      "description":"Overriding environment variables that are reserved by AWS
 Lambda might lead to unexpected behavior or failure of the Lambda function.",
      "findingArn":"arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
      "firstObservedAt":"Aug 8, 2023, 7:33:58 PM",
      "lastObservedAt":"Dec 7, 2023, 10:14:45 PM",
      "remediation":{
         "recommendation":{
            "text":"Your code attempts to override an environment variable that is
 reserved by the Lambda runtime environment. This can lead to unexpected behavior
 and might break the execution of your Lambda function.\n\n[Learn more](https://
docs.aws.amazon.com/lambda/latest/dg/configuration-envvars.html#configuration-
envvars-runtime)"
         }
      },
      "resources":[
         {
            "details":{
               "awsLambdaFunction":{
                  "architectures":[
                     "X86_64"
                  ],
                  "codeSha256":"2mtfH+CgubesG6NYpb2zEqBja5WN6FfbH4AAYDuF8RE=",
                  "executionRoleArn":"arn:aws:iam::193043430472:role/service-role/
code-finding-role-7jgg3wan",
                  "functionName":"code-finding",
                  "lastModifiedAt":"Dec 7, 2023, 10:12:48 PM",
                  "packageType":"ZIP",
                  "runtime":"PYTHON_3_7",
                  "version":"$LATEST"
               }
            },
            "id":"arn:aws:lambda:us-east-1:193043430472:function:code-finding:
$LATEST",
            "partition":"aws",
            "region":"us-east-1",
```

```
            "type":"AWS_LAMBDA_FUNCTION"
         }
      ],
      "severity":"HIGH",
      "status":"ACTIVE",
      "title":"Overriding environment variables that are reserved by AWS Lambda
 might lead to unexpected behavior.",
      "type":"CODE_VULNERABILITY",
      "updatedAt":"Dec 7, 2023, 10:14:45 PM"
   }
}
```


> **Note**
>
> O valor detalhado retorna os detalhes do JSON de uma única descoberta como um objeto. Ele não retorna toda a sintaxe de resposta das descobertas, que oferece suporte a várias descobertas em uma matriz.

# Exemplo de esquema completo de eventos de verificação inicial do Amazon Inspector

A seguir está um exemplo do esquema de eventos de um EventBridge evento do Amazon Inspector para concluir uma verificação inicial. Esse evento é criado quando o Amazon Inspector conclui uma verificação inicial de um dos seus recursos.

Os campos a seguir identificam um evento inicial de conclusão da verificação:

- O campo `detail-type` está definido como `Inspector2 Scan`.
- O objeto `detail` contém um objeto `finding-severity-counts` que detalha o número de descobertas nas categorias de severidade aplicáveis como `CRITICAL`, `HIGH` e `MEDIUM`.

Selecione entre as opções para consultar diferentes esquemas de eventos de verificação inicial por tipo de recurso.

### Amazon EC2 instance initial scan


```
{
    "version": "0",
    "id": "28a46762-6ac8-6cc4-4f55-bc9ab99af928",
    "detail-type": "Inspector2 Scan",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T22:52:35Z",
    "region": "us-east-1",
    "resources": [
        "i-087d63509b8c97098"
    ],
    "detail": {
        "scan-status": "INITIAL_SCAN_COMPLETE",
        "finding-severity-counts": {
            "CRITICAL": 0,
            "HIGH": 0,
            "MEDIUM": 0,
            "TOTAL": 0
        },
        "instance-id": "i-087d63509b8c97098",
        "version": "1.0"
    }
}
```


### Amazon ECR image initial scan


```
{
    "version": "0",
    "id": "fdaa751a-984c-a709-44f9-9a9da9cd3606",
    "detail-type": "Inspector2 Scan",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T23:15:18Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ecr:us-east-1:111122223333:repository/inspector2"
    ],
    "detail": {
```

```
        "scan-status": "INITIAL_SCAN_COMPLETE",
        "repository-name": "arn:aws:ecr:us-east-1:111122223333:repository/
inspector2",
        "finding-severity-counts": {
            "CRITICAL": 0,
            "HIGH": 0,
            "MEDIUM": 0,
            "TOTAL": 0
        },
        "image-digest":
 "sha256:965fbcae990b0467ed5657caceaec165018ef44a4d2d46c7cdea80a9dff0d1ea",
        "image-tags": [
            "ubuntu22"
        ],
        "version": "1.0"
    }
}
```

## Lambda function initial scan

```
{
  "version": "0",
  "id": "4f290a7c-361b-c442-03c8-a629f6f20d6c",
  "detail-type": "Inspector2 Scan",
  "source": "aws.inspector2",
  "account": "111122223333",
  "time": "2023-02-23T18:06:03Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:lambda:us-west-2:111122223333:function:lambda-example:$LATEST"
  ],
  "detail": {
    "scan-status": "INITIAL_SCAN_COMPLETE",
    "finding-severity-counts": {
      "CRITICAL": 0,
      "HIGH": 0,
      "MEDIUM": 0,
      "TOTAL": 0
    },
    "version": "1.0"
```

```
  }
}
```

# Exemplo de esquema de eventos de cobertura do Amazon Inspector

A seguir está um exemplo do esquema de eventos de um EventBridge evento do Amazon Inspector para cobertura. Esse evento é criado quando a cobertura de verificação do Amazon Inspector para um recurso é alterada. Os campos a seguir identificam um evento de cobertura:

- O campo `detail-type` está definido como `Inspector2 Coverage`.
- O objeto `detail` contém um objeto `scanStatus` que indica o novo status de verificação do recurso.

```
{
    "version": "0",
    "id": "000adda5-0fbf-913e-bc0e-10f0376412aa",
    "detail-type": "Inspector2 Coverage",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T22:51:39Z",
    "region": "us-east-1",
    "resources": [
        "i-087d63509b8c97098"
    ],
    "detail": {
        "scanStatus": {
            "reason": "UNMANAGED_EC2_INSTANCE",
            "statusCodeValue": "INACTIVE"
        },
        "scanType": "PACKAGE",
        "eventTimestamp": "2023-01-20T22:51:35.665501Z",
        "version": "1.0"
    }
}
```

# Integrar verificações do Amazon Inspector ao pipeline de CI/CD

Você pode integrar verificações de imagens de contêiner do Amazon Inspector diretamente do pipeline de CI/CD para verificar vulnerabilidades de software e fornecer relatórios no final da compilação. Os relatórios de vulnerabilidade gerados pelo Amazon Inspector permitem investigar e corrigir riscos antes da implantação.

A integração CI/CD do Amazon Inspector utiliza uma combinação do Amazon Inspector SBOM Generator e da API Amazon Inspector Scan para produzir relatórios de vulnerabilidade para as imagens de contêiner. O Amazon Inspector SBOM Generator cria uma lista de materiais de software (SBOM) usando imagem de contêiner fornecida, e a API Amazon Inspector Scan verifica essa SBOM e cria um relatório detalhado das vulnerabilidades detectadas.

Você pode obter uma integração de CI/CD com o Amazon Inspector por meio dos plug-ins do Amazon Inspector criados especificamente para soluções individuais de CI/CD e disponíveis no marketplace, ou você pode criar a própria integração de digitalização personalizada.

Tópicos



## Integração de plug-in

O Amazon Inspector fornece plug-ins para soluções de CI/CD compatíveis. Você pode instalar os plug-ins dos respectivos marketplaces e usar para adicionar o Amazon Inspector Scans como uma etapa de criação no pipeline. A etapa de criação do plug-in executa o Amazon Inspector SBOM Generator na imagem fornecida e a API Amazon Inspector Scan no SBOM gerado.

Veja seguir uma visão geral de como funciona uma integração de CI/CD do Amazon Inspector por meio de plug-ins:

1. Você configura um Conta da AWS para permitir o acesso à API Amazon Inspector Scan. Para obter instruções, consulte Configurando uma AWS conta para usar a integração CI/CD do Amazon Inspector.
2. Você instala o plug-in Amazon Inspector do marketplace.
3. Você instala e configura o binário do Amazon Inspector SBOM Generator. Para obter instruções, consulte Amazon Inspector SBOM Generator.
4. Você adiciona o Amazon Inspector Scans como uma etapa de criação no pipeline de CI/CD e configura a verificação.
5. Ao executar uma compilação, o plug-in usa a imagem do contêiner como entrada e executa o Amazon Inspector SBOM Generator na imagem para gerar um SBOM compatível com CycloneDX.
6. A partir daí, o plug-in envia o SBOM gerado para um endpoint da API Amazon Inspector Scan, que avalia cada componente do SBOM em busca de vulnerabilidades.
7. Com a resposta da API Amazon Inspector Scan, é criado um relatório de vulnerabilidade nos formatos CSV, SBOM JSON e HTML. O relatório contém detalhes sobre todas as vulnerabilidades encontradas pelo Amazon Inspector.

### Soluções CI/CD compatíveis

Atualmente, o Amazon Inspector é compatível com as seguintes soluções de CI/CD. Para obter instruções completas sobre como configurar a integração de CI/CD usando um plug-in, selecione o plug-in para a solução de CI/CD:

- Plug-in Jenkins
- Plug-in do TeamCity

## Integração personalizada

Se o Amazon Inspector não fornecer plug-ins para a solução de CI/CD, você poderá criar a própria integração personalizada de CI/CD ao combinar o Amazon Inspector SBOM Generator e a API Amazon Inspector Scan. Você também pode usar uma integração personalizada para ajustar as verificações usando as opções disponíveis no Amazon Inspector SBOM Generator.

Veja a seguir uma visão geral de como funciona uma integração personalizada de CI/CD do Amazon Inspector:

1. Você configura um Conta da AWS para permitir o acesso à API Amazon Inspector Scan. Para obter instruções, consulte Configurando uma AWS conta para usar a integração CI/CD do Amazon Inspector.
2. Você instala e configura o binário do Amazon Inspector SBOM Generator. Para obter instruções, consulte Amazon Inspector SBOM Generator.
3. Você usa o Amazon Inspector SBOM Generator para gerar um SBOM compatível com o CycloneDX para a imagem de contêiner.
4. Você usa a API Amazon Inspector Scan no SBOM gerado para criar um relatório de vulnerabilidade.

Para obter instruções sobre como configurar uma integração personalizada, consulte Criar a própria integração personalizada de pipeline de CI/CD com o Amazon Inspector Scan.

# Configurando uma AWS conta para usar a integração CI/CD do Amazon Inspector

Você deve se inscrever para usar Conta da AWS a integração CI/CD do Amazon Inspector. Eles Conta da AWS devem ter uma função do IAM que conceda ao seu pipeline acesso à API do Amazon Inspector Scan.

Conclua as tarefas nos tópicos a seguir para se inscrever Conta da AWS, criar um usuário administrador e configurar uma função do IAM para integração de CI/CD.

> **Note**
>
> Se você já se inscreveu em um Conta da AWS, você pode pular paraConfigurar um perfil do IAM para integração de CI/CD.

Tópicos

- Inscreva-se para um Conta da AWS
- Crie um usuário administrador
- Configurar um perfil do IAM para integração de CI/CD

## Inscreva-se para um Conta da AWS

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

Para se inscrever em um Conta da AWS

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

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

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

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

## Crie um usuário administrador

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

Proteja seu Usuário raiz da conta da AWS

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

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

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

Crie um usuário administrador

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No Centro de Identidade do IAM, conceda acesso administrativo a um usuário administrativo.

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

Login como usuário administrativo

- Para fazer login com seu usuário IAM Identity Center, use a URL de login enviada ao seu endereço de e-mail quando você criou o usuário IAM Identity Center user.

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

## Configurar um perfil do IAM para integração de CI/CD

Para integrar a verificação do Amazon Inspector ao pipeline de CI/CD, você precisa criar uma política do IAM que permita acesso à API Amazon Inspector Scan que verifica a lista de materiais de software (SBOMs). Em seguida, você pode anexar essa política ao perfil do IAM que sua conta pode assumir para executar a API Amazon Inspector Scan.

1. Faça login AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação do console do IAM, selecione Políticas e Criar políticas.
3. Em Policy Editor selecione JSON e cole a seguinte instrução:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
```

```
            "Effect": "Allow",
            "Action": "inspector-scan:ScanSbom",
            "Resource": "*"
        }
    ]
}
```

4. Selecione Next (Próximo).
5. Dê um nome à política, por exemplo `InspectorCICDscan-policy`, adicione uma descrição opcional e selecione Criar política. Essa política será anexada à função que você criará nas próximas etapas.
6. No painel de navegação do console do IAM, selecione Funções e selecione Criar nova função.
7. Em Tipo de entidade confiável, selecione Política de confiança personalizada e insira a seguinte política JSON:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{ACCOUNT_ID}:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

8. Selecione Next (Próximo).
9. Na página Adicionar permissões, procure e selecione a política criada anteriormente, depois selecione Próximo.
10. Dê um nome ao perfil, por exemplo `InspectorCICDscan-role`, adicione uma descrição opcional e selecione `Create Role`.

# Amazon Inspector SBOM Generator

O Amazon Inspector SBOM Generator (Sbomgen) é uma ferramenta binária que produz uma lista de materiais de software (SBOM) para uma imagem de contêiner. SBOM é um inventário coletado do software instalado em um sistema.

O Sbomgen funciona verificando arquivos que contêm informações sobre pacotes instalados. Se um desses arquivos for encontrado, a ferramenta extrairá nomes de pacotes, versões e outros metadados. Esses metadados do pacote são transformados em um CycloneDX SBOM.

O Sbomgen pode ser usado como uma ferramenta independente para fornecer o CycloneDX SBOM como um arquivo ou como STDOUT. Ele também é usado como parte da integração CI/CD do Amazon Inspector, que verifica imagens de contêiner automaticamente como parte do pipeline de implantação. Para ter mais informações, consulte Integrar verificações do Amazon Inspector ao pipeline de CI/CD.

## Pacotes e formatos de imagem compatíveis

No momento, o Sbomgen pode coletar inventário dos seguintes tipos de pacotes:

- Alpine APK
- Debian / Ubuntu DPKG
- Red Hat RPM
- Pacotes Go pelo `go.mod` e `go mod cache`
- Pacotes Java pelo `pom.properties`
- Pacotes Node.js pelos arquivos `package.json` dentro de `node_modules`
- Pacotes C# via arquivos Nuget (`.deps.json` ,`csproj`, `Packages.config`, packages.lock.json)
- PHP pelo `installed.json` e `composer.lock`
- Pacotes Python pelos arquivos `requirements.txt`, `Pipfile.lock`, `poetry.lock` e `egg/wheel`
- Pacotes Ruby pelo `Gemfile.lock`, `.gemspec` e gems instaladas no mundo todo
- Pacotes Rust pelo `Cargo.lock` e `Cargo.toml`

O Sbomgen é compatível com os seguintes formatos de manifesto de imagem de contêiner para imagens:

- Manifesto de imagem OCI
- Manifesto de imagem do Docker versão 2, esquema 2
- Manifesto de imagem do Docker versão 2, esquema 1
- Manifesto de imagem do Docker versão 1

> **Important**
>
> O Sbomgen não conseguirá verificar imagens de contêiner se o tamanho for superior a 5 GB, tiver mais de 60 camadas ou tiver mais de 2.000 pacotes instalados.

## Instalar o Amazon Inspector SBOM Generator (Sbomgen)

O Sbomgen está disponível apenas para sistemas operacionais Linux. Se você estiver usando para analisar imagens de contêiner, deverá ter um serviço de contêiner instalado, como Docker, Podman ou containerd.

Para obter melhor performance, recomendamos executar o binário em um sistema com estas especificações mínimas de hardware:

- CPU de 4 núcleos
- RAM de 8 GB

Para instalar o Sbomgen

1. Faça download do arquivo zip Sbomgen do URL correto para a arquitetura:

   Linux AMD64:

   https://amazon-inspector-sbomgen.s3.amazonaws.com/latest/linux/amd64/inspector-sbomgen.zip

   Linux ARM64:

   https://amazon-inspector-sbomgen.s3.amazonaws.com/latest/linux/arm64/inspector-sbomgen.zip
2. Descompacte o download usando o seguinte comando:

```
unzip inspector-sbomgen.zip
```

3. Verifique os seguintes arquivos no arquivo:

   - `inspector-sbomgen`: este é o binário que você executará para gerar SBOMs.
   - `README.txt`: esta é a documentação destinada ao uso do Sbomgen.
   - `LICENSE.txt`: este arquivo contém a licença do software do Sbomgen.
   - `licenses`: esta pasta contém informações de licença dos pacotes de terceiros usados pelo Sbomgen.
   - `checksums.txt`: este arquivo fornece hashes do binário Sbomgen.
   - `sbom.json`: este é um CycloneDX SBOM referente ao binário Sbomgen.
4. (Opcional) Verifique a autenticidade e integridade do binário usando o seguinte comando:

   ```
   sha256sum < inspector-sbomgen
   ```

   - Compare os resultados com o conteúdo do arquivo `checksums.txt`.
5. Conceda permissões executáveis ao binário usando o seguinte comando:

   ```
   chmod +x inspector-sbomgen
   ```
6. Verifique se o Sbomgen foi instalado com sucesso usando o seguinte comando:

   ```
   ./inspector-sbomgen --version
   ```

   Você deverá ver um resultado semelhante a este:

   ```
   Version: 1.X.X
   ```

## Usar o Sbomgen

Você pode usar o Sbomgen para gerar um SBOM para imagens de contêiner.

Você também pode personalizar os resultados da geração do SBOM por meio de opções como exclusão de arquivos específicos ou definição de quais pacotes a ferramenta deve verificar. Para obter exemplos desses casos de uso e muito mais, execute o seguinte comando:

```
./inspector-sbomgen list-examples
```

Para gerar um SBOM para uma imagem de contêiner e enviar o resultado para um arquivo

Neste exemplo, substitua *image:tag* pelo ID da imagem e *output_path.json* pelo caminho onde salvará a saída:

```
./inspector-sbomgen container --image image:tag -o output_path.json
```

## Autenticar registros privados usando o Sbomgen

Você pode gerar um SBOM usando os contêineres hospedados em registros privados, fornecendo credenciais de autenticação de registro privado. Você pode fornecer credenciais de várias maneiras: pelas credenciais armazenadas em cache, por método interativo ou não interativo, em que as credenciais são fornecidas como variáveis de ambiente antes de executar o Sbomgen.

Autenticar usando credenciais armazenadas em cache (recomendado)

1. O Sbomgen tentará usar credenciais armazenadas em cache se estiverem disponíveis no agente. Para esse método, primeiro faça autenticação no registro do contêiner. Por exemplo, se estiver usando o Docker, você poderá fazer a autenticação no registro usando o comando Docker `login`:

   ```
   docker login
   ```

2. Após a autenticação no registro privado, você poderá usar o Sbomgen em uma imagem de contêiner nesse registro. Para usar o exemplo a seguir, substitua *image:tag* pelo nome da imagem a ser digitalizada:

   ```
   ./inspector-sbomgen container --image image:tag
   ```

Autenticar usando o método interativo

- Nesse método, você fornece o nome de usuário como parâmetro e o Sbomgen solicitará uma senha segura quando necessário. Para usar o exemplo a seguir, substitua *image:tag* pelo nome da imagem a ser verificada e *your_username* por um nome de usuário que tenha acesso a essa imagem:

  ```
  ./inspector-sbomgen container --image image:tag --username
  your_username
  ```

Autenticar usando método não interativo

- Para usar esse método, você deve armazenar a senha ou token de registro em um arquivo com formato .txt que só possa ser lido pelo usuário atual. O arquivo de texto deve conter apenas a senha ou token em uma única linha. Para usar o exemplo a seguir, substitua *your_username* pelo nome de usuário, substitua o *password.txt* pelo arquivo que contém senha ou token e substitua *image:tag* pelo nome da imagem a ser verificada:

```
INSPECTOR_SBOMGEN_USERNAME=your_username\
INSPECTOR_SBOMGEN_PASSWORD=`cat password.txt` \
./inspector-sbomgen container --image image:tag
```

## Exemplos de saídas de Sbomgen

Veja a seguir um exemplo de SBOM para uma imagem de contêiner relacionada usando o Sbomgen.

Imagem do contêiner SBOM


```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.5",
  "serialNumber": "urn:uuid:828875ef-8c32-4777-b688-0af96f3cf619",
  "version": 1,
  "metadata": {
    "timestamp": "2023-11-17T21:36:38Z",
    "tools": [
      {
        "vendor": "Amazon Web Services, Inc. (AWS)",
        "name": "Amazon Inspector SBOM Generator",
        "version": "1.0.0",
        "hashes": [
          {
            "alg": "SHA-256",
            "content":
 "10ab669cfc99774786301a745165b5957c92ed9562d19972fbf344d4393b5eb1"
          }
        ]
      }
    ],
    "component": {
      "bom-ref": "comp-1",
```

```
      "type": "container",
      "name": "fedora:latest",
      "properties": [
        {
          "name": "amazon:inspector:sbom_generator:image_id",
          "value":
 "sha256:c81c8ae4dda7dedc0711daefe4076d33a88a69a28c398688090c1141eff17e50"
        },
        {
          "name": "amazon:inspector:sbom_generator:layer_diff_id",
          "value":
 "sha256:eddd0d48c295dc168d0710f70364581bd84b1dda6bb386c4a4de0b61de2f2119"
        }
      ]
    }
  },
  "components": [
    {
      "bom-ref": "comp-2",
      "type": "library",
      "name": "dnf",
      "version": "4.18.0",
      "purl": "pkg:pypi/dnf@4.18.0",
      "properties": [
        {
          "name": "amazon:inspector:sbom_generator:source_file_scanner",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_package_collector",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_path",
          "value": "/usr/lib/python3.12/site-packages/dnf-4.18.0.dist-info/METADATA"
        },
        {
          "name": "amazon:inspector:sbom_generator:is_duplicate_package",
          "value": "true"
        },
        {
          "name": "amazon:inspector:sbom_generator:duplicate_purl",
          "value": "pkg:rpm/fedora/python3-dnf@4.18.0-2.fc39?
arch=noarch&distro=39&epoch=0"
```

```
        }
      ]
    },
    {
      "bom-ref": "comp-3",
      "type": "library",
      "name": "libcomps",
      "version": "0.1.20",
      "purl": "pkg:pypi/libcomps@0.1.20",
      "properties": [
        {
          "name": "amazon:inspector:sbom_generator:source_file_scanner",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_package_collector",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_path",
          "value": "/usr/lib64/python3.12/site-packages/libcomps-0.1.20-py3.12.egg-
info/PKG-INFO"
        },
        {
          "name": "amazon:inspector:sbom_generator:is_duplicate_package",
          "value": "true"
        },
        {
          "name": "amazon:inspector:sbom_generator:duplicate_purl",
          "value": "pkg:rpm/fedora/python3-libcomps@0.1.20-1.fc39?
arch=x86_64&distro=39&epoch=0"
        }
      ]
    }
  ]
}
```

# Criar a própria integração personalizada de pipeline de CI/CD com o Amazon Inspector Scan

Recomendamos usar os plug-ins de CI/CD do Amazon Inspector se eles estiverem disponíveis no marketplace de CI/CD. Consulte Soluções CI/CD compatíveis para ver uma lista dos plug-ins disponíveis.

Se o Amazon Inspector não fornecer plug-ins para a solução de CI/CD, você poderá criar a própria integração personalizada de CI/CD ao combinar o Amazon Inspector SBOM Generator e a API Amazon Inspector Scan. Você também pode usar uma integração personalizada para ajustar as verificações por meio das opções disponíveis no Amazon Inspector SBOM Generator.

Para configurar a própria integração personalizada

1. Configure um Conta da AWS para permitir o acesso à API do Amazon Inspector Scan. Para obter instruções, consulte Configurando uma AWS conta para usar a integração CI/CD do Amazon Inspector.
2. Instale e configure o binário do Amazon Inspector SBOM Generator. Para obter instruções, consulte Instalar o Amazon Inspector SBOM Generator (Sbomgen).
3. Use o SBOM Generator para criar um arquivo SBOM para uma imagem de contêiner que você deseja verificar. Para usar o exemplo a seguir, substitua *image:id* pelo nome da imagem a ser verificada e *sbom_path.json* pelo local para salvar a saída do SBOM:

   ```
   ./inspector-sbomgen container –image image:id -o sbom_path.json
   ```

4. Considere usar a API `inspector-scan` para verificar o SBOM gerado e fornecer um relatório de vulnerabilidade. Para usar o exemplo a seguir, substitua *sbom_path.json* pelo caminho do arquivo para um arquivo SBOM válido compatível com o CycloneDX. Em seguida, substitua *ENDPOINT* pelo endpoint da API para o Região da AWS qual você está autenticado no momento e substitua *REGION pela região* correspondente. Consulte Endpoints para API Amazon Inspector Scan para ver uma lista completa de regiões e endpoints.

   ```
   aws inspector-scan scan-sbom --sbom file://sbom_path.json --endpoint
   "ENDPOINT" --region REGION
   ```

# Formatos de saída da API

A API Amazon Inspector Scan pode gerar um relatório de vulnerabilidade no formato CycloneDX 1.5 ou no formato JSON de descobertas do Amazon Inspector. O padrão pode ser alterado usando o sinalizador `--output-format`.

Exemplo de saída no formato CycloneDX 1.5


```
{
  "status": "SBOM parsed successfully, 1 vulnerabilities found",
  "sbom": {
    "bomFormat": "CycloneDX",
    "specVersion": "1.5",
    "serialNumber": "urn:uuid:0077b45b-ff1e-4dbb-8950-ded11d8242b1",
    "metadata": {
      "properties": [
        {
          "name": "amazon:inspector:sbom_scanner:critical_vulnerabilities",
          "value": "1"
        },
        {
          "name": "amazon:inspector:sbom_scanner:high_vulnerabilities",
          "value": "0"
        },
        {
          "name": "amazon:inspector:sbom_scanner:medium_vulnerabilities",
          "value": "0"
        },
        {
          "name": "amazon:inspector:sbom_scanner:low_vulnerabilities",
          "value": "0"
        }
      ],
      "tools": [
        {
          "name": "CycloneDX SBOM API",
          "vendor": "Amazon Inspector",
          "version": "empty:083c9b00:083c9b00:083c9b00"
        }
      ],
      "timestamp": "2023-06-28T14:15:53.760Z"
    },
    "components": [
```

```
      {
        "bom-ref": "comp-1",
        "type": "library",
        "name": "log4j-core",
        "purl": "pkg:maven/org.apache.logging.log4j/log4j-core@2.12.1",
        "properties": [
          {
            "name": "amazon:inspector:sbom_scanner:path",
            "value": "/home/dev/foo.jar"
          }
        ]
      }
    ],
    "vulnerabilities": [
      {
        "bom-ref": "vuln-1",
        "id": "CVE-2021-44228",
        "source": {
          "name": "NVD",
          "url": "https://nvd.nist.gov/vuln/detail/CVE-2021-44228"
        },
        "references": [
          {
            "id": "SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720",
            "source": {
              "name": "SNYK",
              "url": "https://security.snyk.io/vuln/SNYK-JAVA-
ORGAPACHELOGGINGLOG4J-2314720"
            }
          },
          {
            "id": "GHSA-jfh8-c2jp-5v3q",
            "source": {
              "name": "GITHUB",
              "url": "https://github.com/advisories/GHSA-jfh8-c2jp-5v3q"
            }
          }
        ],
        "ratings": [
          {
            "source": {
              "name": "NVD",
              "url": "https://www.first.org/cvss/v3-1/"
            },
```

```
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
          },
          {
            "source": {
              "name": "NVD",
              "url": "https://www.first.org/cvss/v2/"
            },
            "score": 9.3,
            "severity": "critical",
            "method": "CVSSv2",
            "vector": "AC:M/Au:N/C:C/I:C/A:C"
          },
          {
            "source": {
              "name": "EPSS",
              "url": "https://www.first.org/epss/"
            },
            "score": 0.97565,
            "severity": "none",
            "method": "other",
            "vector": "model:v2023.03.01,date:2023-06-27T00:00:00+0000"
          },
          {
            "source": {
              "name": "SNYK",
              "url": "https://security.snyk.io/vuln/SNYK-JAVA-
ORGAPACHELOGGINGLOG4J-2314720"
            },
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H"
          },
          {
            "source": {
              "name": "GITHUB",
              "url": "https://github.com/advisories/GHSA-jfh8-c2jp-5v3q"
            },
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
```

```
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
          }
        ],
        "cwes": [
          400,
          20,
          502
        ],
        "description": "Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security
 releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages,
 and parameters do not protect against attacker controlled LDAP and other JNDI related
 endpoints. An attacker who can control log messages or log message parameters can
 execute arbitrary code loaded from LDAP servers when message lookup substitution is
 enabled. From log4j 2.15.0, this behavior has been disabled by default. From version
 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely
 removed. Note that this vulnerability is specific to log4j-core and does not affect
 log4net, log4cxx, or other Apache Logging Services projects.",
        "advisories": [
          {
            "url": "https://www.intel.com/content/www/us/en/security-center/advisory/
intel-sa-00646.html"
          },
          {
            "url": "https://support.apple.com/kb/HT213189"
          },
          {
            "url": "https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-
cve-2021-44228-apache-log4j2/"
          },
          {
            "url": "https://logging.apache.org/log4j/2.x/security.html"
          },
          {
            "url": "https://www.debian.org/security/2021/dsa-5020"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf"
          },
          {
            "url": "https://www.oracle.com/security-alerts/alert-cve-2021-44228.html"
          },
          {
            "url": "https://www.oracle.com/security-alerts/cpujan2022.html"
          },
```

```
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf"
          },
          {
            "url": "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/M5CSVUNV4HWZZXGOKNSK6L7RPM7BOKIB/"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf"
          },
          {
            "url": "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/VU57UJDCFIASIO35GC55JMKSRXJMCDFM/"
          },
          {
            "url": "https://www.oracle.com/security-alerts/cpuapr2022.html"
          },
          {
            "url": "https://twitter.com/kurtseifried/status/1469345530182455296"
          },
          {
            "url": "https://tools.cisco.com/security/center/content/
CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd"
          },
          {
            "url": "https://lists.debian.org/debian-lts-announce/2021/12/msg00007.html"
          },
          {
            "url": "https://www.kb.cert.org/vuls/id/930724"
          }
        ],
        "created": "2021-12-10T10:15:00Z",
        "updated": "2023-04-03T20:15:00Z",
        "affects": [
          {
            "ref": "comp-1"
          }
        ],
        "properties": [
          {
            "name": "amazon:inspector:sbom_scanner:exploit_available",
```

```
            "value": "true"
          },
          {
            "name": "amazon:inspector:sbom_scanner:exploit_last_seen_in_public",
            "value": "2023-03-06T00:00:00Z"
          },
          {
            "name": "amazon:inspector:sbom_scanner:cisa_kev_date_added",
            "value": "2021-12-10T00:00:00Z"
          },
          {
            "name": "amazon:inspector:sbom_scanner:cisa_kev_date_due",
            "value": "2021-12-24T00:00:00Z"
          },
          {
            "name": "amazon:inspector:sbom_scanner:fixed_version:comp-1",
            "value": "2.15.0"
          }
        ]
      }
    ]
  }
}
```

Exemplo de saída no formato do Inspector

```
                        {
  "status": "SBOM parsed successfully, 1 vulnerability found",
  "inspector": {
    "messages": [
      {
        "name": "foo",
        "purl": "pkg:maven/foo@1.0.0", // Will not exist in output if missing in sbom
        "info": "Component skipped: no rules found."
      }
    ],
    "vulnerability_count": {
      "critical": 1,
      "high": 0,
      "medium": 0,
      "low": 0
    },
```

```
    "vulnerabilities": [
      {
        "id": "CVE-2021-44228",
        "severity": "critical",
        "source": "https://nvd.nist.gov/vuln/detail/CVE-2021-44228",
        "related": [
          "SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720",
          "GHSA-jfh8-c2jp-5v3q"
        ],
        "description": "Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security
 releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages,
 and parameters do not protect against attacker controlled LDAP and other JNDI related
 endpoints. An attacker who can control log messages or log message parameters can
 execute arbitrary code loaded from LDAP servers when message lookup substitution is
 enabled. From log4j 2.15.0, this behavior has been disabled by default. From version
 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely
 removed. Note that this vulnerability is specific to log4j-core and does not affect
 log4net, log4cxx, or other Apache Logging Services projects.",
        "references": [
          "https://www.intel.com/content/www/us/en/security-center/advisory/intel-
sa-00646.html",
          "https://support.apple.com/kb/HT213189",
          "https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-
cve-2021-44228-apache-log4j2/",
          "https://logging.apache.org/log4j/2.x/security.html",
          "https://www.debian.org/security/2021/dsa-5020",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf",
          "https://www.oracle.com/security-alerts/alert-cve-2021-44228.html",
          "https://www.oracle.com/security-alerts/cpujan2022.html",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf",
          "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/M5CSVUNV4HWZZXGOKNSK6L7RPM7BOKIB/",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf",
          "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/VU57UJDCFIASIO35GC55JMKSRXJMCDFM/",
          "https://www.oracle.com/security-alerts/cpuapr2022.html",
          "https://twitter.com/kurtseifried/status/1469345530182455296",
          "https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-
sa-apache-log4j-qRuKNEbd",
          "https://lists.debian.org/debian-lts-announce/2021/12/msg00007.html",
          "https://www.kb.cert.org/vuls/id/930724"
        ],
        "created": "2021-12-10T10:15:00Z",
```

```
        "updated": "2023-04-03T20:15:00Z",
        "properties": {
          "cisa_kev_date_added": "2021-12-10T00:00:00Z",
          "cisa_kev_date_due": "2021-12-24T00:00:00Z",
          "cwes": [
            400,
            20,
            502
          ],
          "cvss": [
            {
              "source": "NVD",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H",
              "cvss2_base_score": 9.3,
              "cvss2_base_vector": "AC:M/Au:N/C:C/I:C/A:C"
            },
            {
              "source": "SNYK",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H"
            },
            {
              "source": "GITHUB",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
            }
          ],
          "epss": 0.97565,
          "exploit_available": true,
          "exploit_last_seen_in_public": "2023-03-06T00:00:00Z"
        },
        "affects": [
          {
            "installed_version": "pkg:maven/org.apache.logging.log4j/log4j-
core@2.12.1",
            "fixed_version": "2.15.0",
            "path": "/home/dev/foo.jar"
          }
        ]
      }
```

```
    ]
  }
}
```

# Como usar o plug-in Jenkins do Amazon Inspector

O Jenkins plug-in utiliza o binário do Amazon Inspector SBOM Generator e a API Amazon Inspector Scan para produzir relatórios detalhados no final da sua criação, para que você possa investigar e corrigir riscos antes da implantação.

O Amazon Inspector é um serviço de gerenciamento de vulnerabilidades que escaneia imagens de contêineres em busca de vulnerabilidades do sistema operacional e do pacote de linguagem de programação com base em CVEs.

Usando o Jenkins plug-in do Amazon Inspector, você pode adicionar escaneamentos de vulnerabilidade do Amazon Inspector ao seu pipeline. Jenkins

> **Note**
>
> As varreduras de vulnerabilidade do Amazon Inspector podem ser configuradas para aprovar ou falhar nas execuções do pipeline com base no número e na gravidade das vulnerabilidades detectadas.

Você pode ver a versão mais recente do Jenkins plug-in no Jenkins mercado em https://plugins.jenkins.io/amazon-inspector-image-scanner/.

As etapas a seguir descrevem como configurar o plug-in Amazon Inspector Jenkins.

> **Important**
>
> Antes de concluir as etapas a seguir, você deve atualizar o Jenkins para a versão 2.387.3 ou superior para que o plug-in seja executado.

## Etapa 1. Configurar um Conta da AWS

Configure um Conta da AWS com uma função do IAM que permita o acesso à API Amazon Inspector Scan. Para obter instruções, consulte Configurando uma AWS conta para usar a integração CI/CD do Amazon Inspector.

## Etapa 2. Instale o plug-in Amazon Inspector Jenkins

O procedimento a seguir descreve como instalar o plug-in Jenkins do Amazon Inspector a partir do painel. Jenkins

1. No painel do Jenkins, escolha Gerenciar Jenkins e, em seguida, selecione Gerenciar plug-ins.
2. Escolha Disponível.
3. Na guia Disponível, pesquise Amazon Inspector Scans e, em seguida, instale o plug-in.

## (Opcional) Etapa 3. Adicione credenciais do docker ao Jenkins

> **Note**
>
> Adicione credenciais do docker somente se a imagem do docker estiver em um repositório privado. Caso contrário, ignore essa etapa.

O procedimento a seguir descreve como adicionar credenciais do docker a Jenkins partir do painel. Jenkins

1. No painel do Jenkins, escolha Gerenciar Jenkins, Credenciais e, em seguida, Sistema.
2. Escolha Credenciais globais e, em seguida, Adicionar credenciais.
3. Em Tipo, selecione Nome de usuário com senha.
4. Em Escopo, selecione Global (Jenkins, nós, itens, todos os itens secundários etc.).
5. Insira seus detalhes e, em seguida, escolha OK.

## (Opcional) Etapa 4. Adicionar AWS credenciais

> **Note**
>
> Adicione AWS credenciais somente se quiser se autenticar com base em um usuário do IAM. Caso contrário, ignore essa etapa.

O procedimento a seguir descreve como adicionar AWS credenciais do Jenkins painel.

1. No painel do Jenkins, escolha Gerenciar Jenkins, Credenciais e, em seguida, Sistema.
2. Escolha Credenciais globais e, em seguida, Adicionar credenciais.
3. Em Tipo, selecione Credenciais da AWS.
4. Insira seus detalhes, incluindo a ID da chave de acesso e a chave de acesso secreta, e escolha OK.

## Etapa 5. Adicionar suporte a CSS em um Jenkins script

O procedimento a seguir descreve como adicionar suporte a CSS em um Jenkikns script.

1. Reinicie o Jenkins.
2. No Painel, escolha Gerenciar Jenkins, Nodes, Built-Node e, em seguida, Script Console.
3. Na caixa de texto, adicione a linha `System.setProperty("hudson.model.DirectoryBrowserSupport.CSP", "")` e escolha Executar.

## Etapa 6. Adicione o Amazon Inspector Scan à sua compilação

Você pode adicionar o Amazon Inspector Scan à criação inserindo uma etapa de criação ao projeto ou usando o pipeline declarativo Jenkins.

### Amazon Inspector Digitalize sua compilação adicionando uma etapa de compilação em seu projeto

1. Na página de configuração, role para baixo até Etapas de compilação e escolha Adicionar etapa de compilação. Em seguida, selecione Amazon Inspector Scan.

2. Escolha entre dois métodos de instalação do inspector-sbomgen: Automático ou Manual.

   a. (Opção 1) Escolha Automático para baixar a versão mais recente do inspector-sbomgen. Se você escolher esse método, certifique-se de selecionar a arquitetura da CPU que corresponde ao sistema que executa o plug-in.

   b. (Opção 2) Escolha Manual se quiser configurar o binário do Amazon Inspector SBOM Generator para digitalização. Se você escolher esse método, certifique-se de fornecer o caminho completo para uma versão baixada anteriormente do inspector-sbomgen.

   Para obter mais informações, consulte Instalação do Amazon Inspector SBOM Generator (Sbomgen) no Amazon Inspector SBOM Generator.

3. Faça o seguinte para realizar a configuração da etapa de criação do Amazon Inspector Scan:

   a. Insira o ID da imagem. A imagem pode ser local, remota ou arquivada. Os nomes das imagens devem seguir a convenção de nomenclatura do Docker. Se estiver analisando uma imagem exportada, forneça o caminho para o arquivo tar previsto. Veja os seguintes exemplos de caminhos de ID da imagem:

      i. Para contêineres locais ou remotos: `NAME[:TAG|@DIGEST]`

      ii. Para um arquivo tar: `/path/to/image.tar`

   b. Selecione uma Região da AWS para enviar a solicitação de escaneamento.

   c. (Opcional) Para credenciais do Docker, selecione o nome de usuário Docker. Faça isso apenas se a imagem de contêiner estiver em um repositório privado.

   d. (Opcional) Você pode fornecer os seguintes métodos de AWS autenticação compatíveis:

      i. (Opcional) Para a função IAM, forneça um ARN da função (arn:aws:iam: ::role/). *AccountNumberRoleName*

      ii. (Opcional) Para credenciais da AWS, selecione Id para autenticar com base em um usuário do IAM.

      iii. (Opcional) Em nome AWS do perfil, forneça o nome de um perfil a ser autenticado usando um nome de perfil.

   e. (Opcional) Especifique os Limites de vulnerabilidade por grau. Se o número especificado for excedido durante uma verificação, a construção da imagem falhará. Se todos os valores forem `0`, a compilação será bem-sucedida, independentemente de alguma vulnerabilidade ser encontrada.

4. Selecione Save (Salvar).

## Adicione o Amazon Inspector Scan à sua compilação usando o pipeline declarativo Jenkins

Você pode adicionar o Amazon Inspector Scan à sua compilação usando o pipeline declarativo Jenkins de forma automática ou manual.

Para baixar automaticamente o pipeline declarativo SBOMgen

- Para adicionar o Amazon Inspector Scan a uma compilação, use o seguinte exemplo de sintaxe. Com base na sua arquitetura de sistema operacional preferida do download do Amazon Inspector SBOM Generator, substitua *SBOMGEN_SOURCE* por LinuxAMD64 ou LinuxARM64. *Substitua IMAGE_PATH pelo caminho para sua imagem (como alpine:latest), IAM_ROLE pelo ARN da função do IAM que você configurou na etapa 1 e ID pela sua ID de credencial se estiver usando um repositório privado.* Docker Se desejar, você poderá ativar os limites de vulnerabilidade e especificar valores para cada grau.

```
pipeline {
   agent any
   stages {
       stage('amazon-inspector-image-scanner') {
           steps {
               script {
               step([
               $class:
 'com.amazon.inspector.jenkins.amazoninspectorbuildstep.AmazonInspectorBuilder',
               sbomgenSource: 'SBOMGEN_SOURCE', // this can be linuxAmd64 or linuxArm64
               archivePath: 'IMAGE_PATH',
               awsRegion: 'REGION',
               iamRole: 'IAM ROLE',
               credentialId: 'Id', // provide empty string if image not in private
 repositories
               awsCredentialId: ''AWS ID;',
               awsProfileName: 'Profile Name',
               isThresholdEnabled: false,
               countCritical: 0,
               countHigh: 0,
               countLow: 10,
```

```
                countMedium: 5,
               ])
            }
          }
        }
    }
}
```

Para baixar manualmente o pipeline declarativo SBOMgen

- Para adicionar o Amazon Inspector Scan a uma compilação, use o seguinte exemplo de sintaxe. *Substitua SBOMGEN_PATH pelo caminho para o Amazon Inspector SBOM Generator que você instalou na etapa 3, IMAGE_PATH pelo caminho para sua imagem (como alpine:latest), IAM_ROLE pelo ARN da função IAM que você configurou na etapa 1 e ID pelo seu ID de credencial se você estiver usando um repositório privado.* Docker Se desejar, você poderá ativar os limites de vulnerabilidade e especificar valores para cada grau.

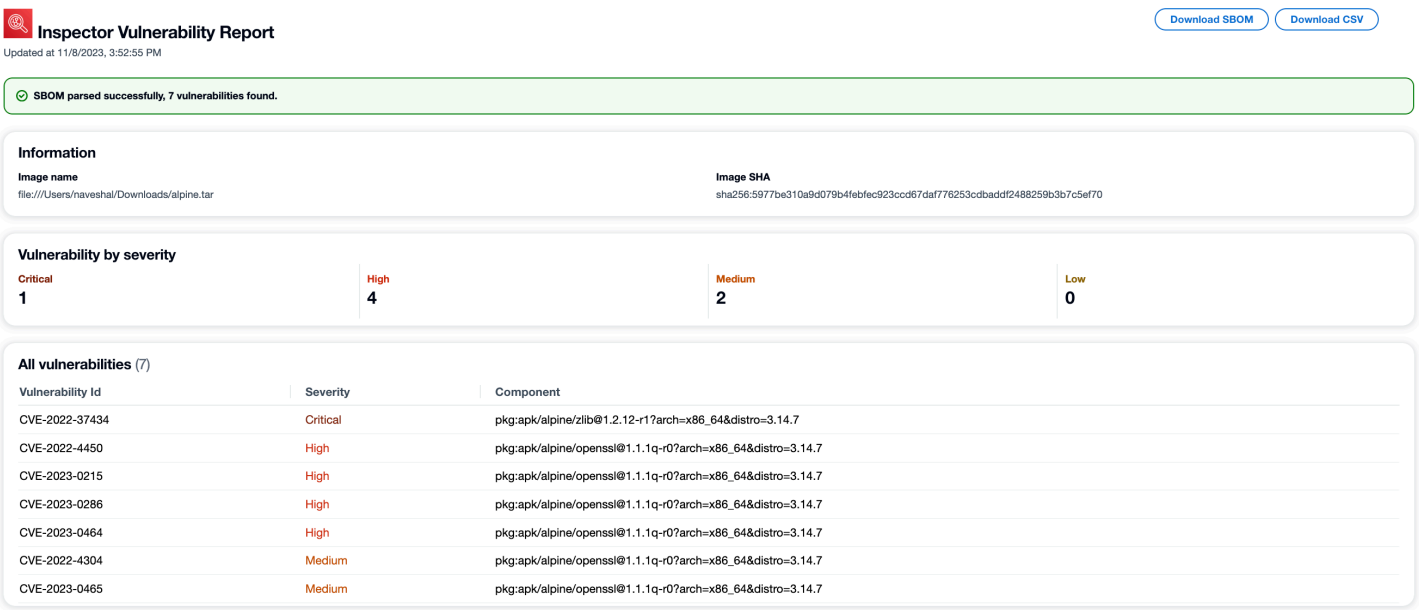
> **Note**
>
> Coloque Sbomgen no diretório Jenkins e forneça o caminho para o diretório Jenkins no plugin (como */opt/folder/arm64/inspector-sbomgen*).

```
pipeline {
    agent any
    stages {
        stage('amazon-inspector-image-scanner') {
            steps {
                script {
                step([
                $class:
 'com.amazon.inspector.jenkins.amazoninspectorbuildstep.AmazonInspectorBuilder',
                sbomgenPath: 'SBOMGEN_PATH',
                archivePath: 'IMAGE_PATH',
                awsRegion: 'REGION',
                iamRole: 'IAM ROLE',
                awsCredentialId: ''AWS ID;',
                credentialId: 'Id;', // provide empty string if image not in private
 repositories
```

```
                awsProfileName: 'Profile Name',
                isThresholdEnabled: false,
                countCritical: 0,
                countHigh: 0,
                countLow: 10,
                countMedium: 5,
              ])
          }
        }
      }
    }
  }
```

## Etapa 7. Veja seu relatório de vulnerabilidade do Amazon Inspector

1. Realize nova compilação do projeto.
2. Depois que a compilação for concluída, selecione um formato de saída nos resultados. Se você selecionar HTML, terá a opção de baixar uma versão JSON, SBOM ou CSV do relatório. Veja a seguir um exemplo de um relatório HTML:




## Solução de problemas

A seguir estão os erros comuns que você pode encontrar ao usar o plug-in Amazon Inspector Scan para. Jenkins

### Falha ao carregar credenciais ou erro de exceção do STS

Erro:

```
InstanceProfileCredentialsProvider(): Failed to load credentials or sts
exception.
```

Resolução

Obtenha `aws_access_key_id` e `aws_secret_access_key` para sua AWS conta. Configure `aws_access_key_id` e `aws_secret_access_key` em `~/.aws/credentials`.

### Erro de caminho do Inspector-SBOMgen

Erro:

```
Exception:com.amazon.inspector.jenkins.amazoninspectorbuildstep.exception.Sbomge
There was an issue running inspector-sbomgen, is /opt/inspector/inspector-
sbomgen the correct path?
```

Resolução:

Conclua o procedimento a seguir para resolver o problema.

1. Coloque a arquitetura correta do sistema operacional Inspector-SBOMgen no Jenkins diretório Para obter mais informações, consulte Amazon Inspector SBOM Generator.
2. Conceda permissões executáveis ao binário usando o seguinte comando:`chmod +x inspector-sbomgen`.
3. Forneça o caminho correto da Jenkins máquina no plug-in, como`/opt/folder/arm64/inspector-sbomgen`.
4. Salve a configuração e execute o Jenkins trabalho.

## Como usar o plug-in TeamCity do Amazon Inspector

O plug-in do Amazon Inspector TeamCity oferece a capacidade de adicionar verificações de vulnerabilidade do Amazon Inspector ao pipeline TeamCity. O plug-in utiliza o binário do Amazon Inspector SBOM Generator e a API Amazon Inspector Scan para gerar relatórios detalhados no final da compilação, para investigar e corrigir os riscos antes da implantação. As verificações também

podem ser configuradas para aprovar ou reprovar execuções do pipeline com base na quantidade e na gravidade das vulnerabilidades detectadas.

O Amazon Inspector é um serviço de gerenciamento de vulnerabilidades oferecido pela AWS que verifica imagens de contêineres para vulnerabilidades do sistema operacional e do pacote de linguagem de programação com base em CVEs. Para obter mais informações sobre a integração do Amazon Inspector com CI/CD, consulte Integrar verificações do Amazon Inspector ao pipeline de CI/CD.

Para obter uma lista dos pacotes e formatos de imagem de contêiner com os quais o plug-in do Amazon Inspector é compatível, consulte Pacotes e formatos de imagem compatíveis.

Você pode ver a versão mais recente do plug-in no TeamCity mercado em https://plugins.jetbrains.com/plugin/23236 - amazon-inspector-scanner. Como alternativa, siga as etapas em cada seção deste documento para configurar o plug-in Amazon Inspector TeamCity:

1. Configure um Conta da AWS.
   - Configure um Conta da AWS com uma função do IAM que permita o acesso à API Amazon Inspector Scan. Para obter instruções, consulte Configurando uma AWS conta para usar a integração CI/CD do Amazon Inspector.
2. Instale o plug-in Amazon Inspector TeamCity.
   a. No painel, acesse Administração > Plugins.
   b. Pesquise por Amazon Inspector Scans.
   c. Instale o plug-in .
3. Instale o Amazon Inspector SBOM Generator.
   - Instale o binário do Amazon Inspector SBOM Generator no diretório do servidor Teamcity. Para obter instruções, consulte Instalar o Amazon Inspector SBOM Generator (Sbomgen).
4. Adicione uma etapa de criação do Amazon Inspector Scan ao projeto.
   a. Na página de configuração, role para baixo até Build Steps, escolha Add build step e selecione Amazon Inspector Scan.
   b. Configure a etapa de criação do Amazon Inspector Scan preenchendo os seguintes detalhes:
      - Adicione um nome de etapa.

- Escolha entre dois métodos de instalação do Amazon Inspector SBOM Generator: Automático ou Manual.
  - Faz o download automático da versão mais recente do Amazon Inspector SBOM Generator com base no seu sistema e na arquitetura da CPU.
  - O manual exige que você forneça um caminho completo para uma versão baixada anteriormente do Amazon Inspector SBOM Generator.

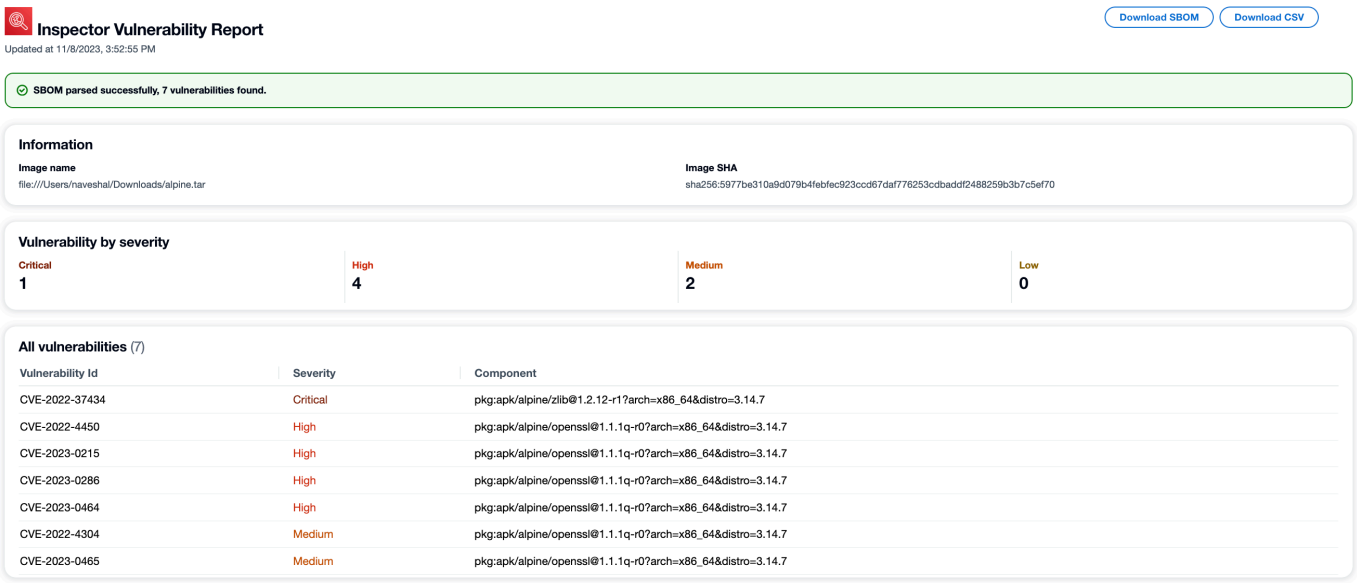
  Para obter mais informações, consulte Instalando o Amazon Inspector SBOM Generator (Sbomgen) no Amazon Inspector SBOM Generator.
- Insira o ID da imagem. A imagem pode ser local, remota ou arquivada. Os nomes das imagens devem seguir a convenção de nomenclatura do Docker. Se estiver analisando uma imagem exportada, forneça o caminho para o arquivo tar previsto. Veja os seguintes exemplos de caminhos de ID da imagem:
  - Para contêineres locais ou remotos: `NAME[:TAG|@DIGEST]`
  - Para um arquivo tar: `/path/to/image.tar`
- Para o perfil do IAM, insira o ARN do perfil configurado na etapa 1.
- Selecione uma Região da AWS para enviar a solicitação de escaneamento.
- (Opcional) Para Autenticação do Docker, insira o Nome de usuário e Senha do Docker. Faça isso apenas se a imagem de contêiner estiver em um repositório privado.
- (Opcional) Para AWS Autenticação, insira o ID da chave de AWS acesso e a chave AWS secreta. Faça isso somente se quiser se autenticar com base nas AWS credenciais.
- (Opcional) Especifique os Limites de vulnerabilidade por grau. Se o número especificado for excedido durante uma verificação, a construção da imagem falhará. Se todos os valores forem `0`, a compilação será bem-sucedida, independentemente do número de vulnerabilidades encontradas.

c. Selecione Save (Salvar).

5. Veja o relatório de vulnerabilidade do Amazon Inspector.

   a. Realize nova compilação do projeto.

   b. Quando a compilação for concluída, selecione um formato de saída nos resultados. Ao selecionar HTML, você pode fazer download da versão JSON SBOM ou CSV do relatório. Este é um exemplo de relatório HTML:




# Namespaces CycloneDX do Amazon Inspector

O Amazon Inspector reservou namespaces CycloneDX e nomes de propriedades para uso com SBOMs produzidos pelo Amazon Inspector SBOM Generator e pela API Amazon Inspector Scan. Essa página documenta todas as propriedades personalizadas de chave/valor que podem ser adicionadas aos componentes nos SBOMs CycloneDX criados usando as ferramentas do Amazon Inspector. Para obter mais informações sobre taxonomias de propriedades do CycloneDX, consulte a documentação oficial.

## Taxonomia de namespace **`amazon:inspector:sbom_scanner`**

O namespace `amazon:inspector:sbom_scanner` é usado pela API Amazon Inspector Scan. Ele tem as seguintes propriedades:

| Propriedade | Descrição |
| --- | --- |
| `amazon:inspector:sbom_scanner:critical_vulnerabilities` | Contagem do número total de vulnerabilidades de gravidade crítica encontradas no SBOM. |
| `amazon:inspector:sbom_scanner:high_vulnerabilities` | Contagem do número total de vulnerabilidades de alta gravidade encontradas no SBOM. |

| Propriedade | Descrição |
| --- | --- |
| `amazon:inspector:sbom_scanner:medium_vulnerabilities` | Contagem do número total de vulnerabilidades de gravidade média encontradas no SBOM. |
| `amazon:inspector:sbom_scanner:low_vulnerabilities` | Contagem do número total de vulnerabilidades de baixa gravidade encontradas no SBOM. |
| `amazon:inspector:sbom_scanner:info` | Fornece contexto de verificação para um determinado componente, por exemplo: “Componente verificado: nenhuma vulnerabilidade encontrada”. |
| `amazon:inspector:sbom_scanner:warning` | Fornece contexto para o motivo pelo qual um determinado componente não foi verificado, por exemplo: “Componente ignorado: nenhum URL fornecido”. |
| `amazon:inspector:sbom_scanner:fixed_version: component_bom_ref` | Fornece a versão fixa do componente indicado para a vulnerabilidade determinada. |
| `amazon:inspector:sbom_scanner:exploit_available` | Indica se uma exploração está disponível para determinada vulnerabilidade. |
| `amazon:inspector:sbom_scanner:exploit_last_seen_in_public` | Indica quando uma exploração foi vista em público pela última vez para uma determinada vulnerabilidade. |
| `amazon:inspector:sbom_scanner:cisa_kev_date_added` | Indica quando a vulnerabilidade foi adicionada ao catálogo de vulnerabilidades conhecidas exploradas do CISA. |
| `amazon:inspector:sbom_scanner:cisa_kev_date_due` | Indica quando a correção da vulnerabilidade é devida de acordo com o catálogo Vulnerabilidades Conhecidas Exploradas da CISA. |
| `amazon:inspector:sbom_scanner:path` | O caminho para o arquivo que gerou as informações do pacote em questão. |

# Taxonomia de namespace **amazon:inspector:sbom_generator**

O namespace `amazon:inspector:sbom_generator` é usado pelo Amazon Inspector SBOM Generator. Ele tem as seguintes propriedades:

| Propriedade | Descrição |
| --- | --- |
| `amazon:inspector:sbom_generator:os_hostname` | O nome do host do sistema que está sendo inventariado. |
| `amazon:inspector:sbom_generator:kernel_name` | O nome do kernel do sistema que está sendo inventariado. |
| `amazon:inspector:sbom_generator:kernel_version` | A versão do kernel do sistema que está sendo inventariado. |
| `amazon:inspector:sbom_generator:cpu_architecture` | A arquitetura de CPU do sistema que está sendo inventariado, como x86_64. |
| `amazon:inspector:sbom_generator:image_id` | O hash do arquivo de configuração da imagem do contêiner, também conhecido como ID da imagem. |
| `amazon:inspector:sbom_generator:layer_diff_id` | O hash da camada de imagem do contêiner descompactada. |
| `amazon:inspector:sbom_generator:source_file_scanner` | O leitor que encontrou o arquivo que contém informações do pacote, por exemplo `/var/lib/dpkg/status` . |
| `amazon:inspector:sbom_generator:source_package_collector` | O coletor que extraiu o nome e a versão do pacote de um arquivo específico. |
| `amazon:inspector:sbom_generator:source_path` | O caminho para o arquivo do qual as informaçõ es do pacote em questão foram extraídas. |
| `amazon:inspector:sbom_generator:is_duplicate_package` | Indica que o pacote em questão foi encontrado por mais de um leitor de arquivo. |

| Propriedade | Descrição |
| --- | --- |
| `amazon:inspector:sbom_generator:go_toolchain` | Indica a versão do compilador Go ou a versão do conjunto de ferramentas usado para produzir um executável Go. |
| `amazon:inspector:sbom_generator:expires_before` | a data anterior à validade do certificado SSL. |
| `amazon:inspector:sbom_generator:expires_after` | a data após a qual o certificado SSL é inválido. |
| `amazon:inspector:sbom_generator:is_expired` | um valor booleano que indica se o certificado SSL expirou. |

# Verificação automatizada de recursos do Amazon Inspector

A verificação sem agente do Amazon Inspector para o Amazon EC2 está em versão prévia. O uso do recurso de verificação sem agente do Amazon EC2 está sujeito à Seção 2 dos Termos de serviço da AWS ("Betas e versões prévias").

O Amazon Inspector usa seu próprio mecanismo de verificação criado especificamente. Esse mecanismo monitora seus recursos em busca de vulnerabilidades de software ou caminhos de rede abertos que podem resultar em workloads comprometidas, uso mal intencionado de recursos ou acesso não autorizado aos seus dados. Quando o Amazon Inspector detecta uma vulnerabilidade, ele cria uma descoberta. As descobertas incluem detalhes associados à detecção para ajudá-lo a corrigir a vulnerabilidade. Analise as descobertas no console do Amazon Inspector e usando a API do Amazon Inspector. Para ter mais informações, consulte Gerenciar descobertas no Amazon Inspector.

Quando ativado, o Amazon Inspector descobre automaticamente todos os recursos elegíveis e inicia verificações contínuas desses recursos. O Amazon Inspector verifica vulnerabilidades de software e exposição não intencional da rede. O Amazon Inspector também executa verificações em resposta a eventos, como a instalação de um novo aplicativo ou patch.

Ao ativar o Amazon Inspector pela primeira vez, sua conta é automaticamente inscrita em todos os tipos de verificação. Os tópicos a seguir abrangem detalhes específicos sobre os tipos de verificação que o Amazon Inspector fornece. O Amazon Inspector categoriza os tipos de verificação com base no tipo de recurso afetado por uma vulnerabilidade. Os tópicos a seguir abordam quais recursos o Amazon Inspector verifica, o que inicia novas verificações para esses recursos e como configurar as verificações para cada tipo de recurso.

Tópicos

Ao ativar o Amazon Inspector pela primeira vez, sua conta é automaticamente inscrita nos seguintes tipos de verificação: escaneamento do Amazon EC2, escaneamento do Amazon ECR, escaneamento padrão do Lambda. O escaneamento de código do Lambda é uma camada opcional do escaneamento de funções do Lambda que você poderá ativar a qualquer momento.

# Visão geral dos tipos de verificação do Amazon Inspector

O Amazon Inspector oferece uma variedade de tipos diferentes de escaneamento focados em tipos de recursos específicos em seu AWS ambiente.

Escaneamento do Amazon EC2

Ao ativar a escaneamento do Amazon EC2, o Amazon Inspector verifica suas instâncias do Amazon EC2 em busca de vulnerabilidades de pacotes de sistemas operacionais e linguagens de programação, além de acessibilidade de rede. O Amazon Inspector verifica a instância do EC2 em busca de vulnerabilidades e exposições comuns (CVE) e problemas de exposição de rede. O Amazon Inspector realiza verificações por meio do agente SSM instalado na instância ou por meio de snapshots de instâncias do Amazon EBS. Para obter mais informações sobre as verificações do Amazon EC2, consulte Verificar as instâncias do Amazon EC2 com o Amazon Inspector.

Escaneamento do Amazon ECR

Quando você ativa o escaneamento do Amazon ECR, o Amazon Inspector converte todos os repositórios de contêineres de escaneamento básico em seu registro privado em escaneamento avançado com escaneamento contínuo. Outra opção é definir essa configuração para verificar somente por push ou para verificar repositórios selecionados por meio de regras de inclusão. Todas as imagens enviadas nos últimos 30 dias ou retiradas nos últimos 90 dias são digitalizadas inicialmente. Por padrão, o Amazon Inspector continua monitorando imagens por um período de 90 dias. Essa configuração pode ser alterada a qualquer momento. Para obter mais informações sobre as verificações do Amazon ECR, consulte Verificar imagens de contêineres do Amazon ECR com o Amazon Inspector.

Escaneamento padrão do Lambda

Ao ativar o escaneamento padrão do Lambda, o Amazon Inspector descobre as funções do Lambda em sua conta e imediatamente começa a verificá-las em busca de vulnerabilidades. O Amazon Inspector verifica novas funções e camadas do Lambda quando elas são implantadas e as verifica novamente quando são atualizadas ou quando novas CVEs (vulnerabilidades e

exposições comuns) são publicadas. Para obter mais informações sobre a verificação da função do Lambda, consulte AWS Lambda Funções de digitalização com o Amazon Inspector.

Escaneamento padrão do Lambda + Escaneamento de código do Lambda

Essa opção pode combinar o escaneamento padrão do Lambda com a escaneamento de código do Lambda. Quando o escaneamento de código do Lambda é ativado, o Amazon Inspector descobre as funções e camadas do Lambda em sua conta e verifica vulnerabilidades de código, dependências de pacotes de aplicativos. O escaneamento de código do Lambda verifica o código do aplicativo personalizado em suas funções do Lambda em busca de vulnerabilidades de código. Esses dois tipos de verificação devem ser ativados juntos. Para obter mais informações, consulte Escaneamento de código do Lambda do Amazon Inspector.

## Ativar um tipo de verificação

Ative um novo tipo de verificação do Amazon Inspector a qualquer momento. Depois de ativar um tipo de escaneamento, o Amazon Inspector começará imediatamente a escanear recursos elegíveis para esse tipo de escaneamento. Para obter uma visão geral dos tipos de verificação disponíveis, consulte Visão geral dos tipos de verificação do Amazon Inspector. A seguir, descrevemos o que acontece ao ativar cada tipo de verificação pela primeira vez:

- Escaneamento do Amazon EC2: ao ativar do Amazon Inspector o Amazon EC2 verifica uma conta, o Amazon Inspector verifica todas as instâncias elegíveis em sua conta em busca de vulnerabilidades de pacotes e problemas de acessibilidade de rede. O plug-in Amazon Inspector SSM está instalado em todos os seus hosts gerenciados pelo SSM. Windows Para ter mais informações, consulte Verificação das instâncias do Windows.. Além disso, o Amazon Inspector cria as seguintes associações SSM na sua conta:
  - `InspectorDistributor-do-not-delete`
  - `InspectorInventoryCollection-do-not-delete`
  - `InspectorLinuxDistributor-do-not-delete`
  - `InvokeInspectorLinuxSsmPlugin-do-not-delete`
  - `InvokeInspectorSsmPlugin-do-not-delete`.
- Escaneamento do Amazon ECR: ao ativar o escaneamento de imagens de contêineres do Amazon ECR para uma conta, o tipo de escaneamento do Amazon ECR para repositórios privados nessa conta muda de Escaneamento básico com o Amazon ECR, para Escaneamento avançado com o Amazon Inspector. Em seguida, todas as imagens de contêineres elegíveis do Amazon

ECR enviadas nos últimos 30 dias ou retiradas nos últimos 90 dias são escaneadas em busca de vulnerabilidades de pacotes. Além disso, a duração da redigitalização do Amazon ECR está definida para 90 dias para a data de envio e extração da imagem.

- Escaneamento padrão do Lambda: ao ativar o escaneamento padrão do Lambda em uma conta, todas as funções do Lambda em sua conta que foram invocadas ou atualizadas nos últimos 90 dias são verificadas em busca de vulnerabilidades do pacote. Além disso, um canal vinculado ao CloudTrail serviço é criado em sua conta.
- Escaneamento padrão do Lambda + Escaneamento de código do Lambda: esses tipos de verificação da função do Lambda são ativados juntos. Ao ativar o escaneamento de código do Lambda em uma conta, todas as funções do Lambda em sua conta que foram invocadas ou atualizadas nos últimos 90 dias são verificadas em busca de vulnerabilidades de código.

## Habilitar as verificações

Se você for o administrador delegado do Amazon Inspector em AWS uma organização, você pode habilitar vários tipos de escaneamento do Amazon Inspector para várias contas em várias regiões automaticamente usando um script de shell desenvolvido pelo Amazon Inspector inspector2- on. enablement-with-cli GitHub Caso contrário, para concluir este procedimento para um ambiente de várias contas por meio do console, conclua as etapas a seguir enquanto estiver conectado como administrador delegado do Amazon Inspector.

Console

Para ativar as verificações

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região em que você deseja ativar um novo tipo de digitalização.
3. No painel de navegação, escolha Gerenciamento de contas.
4. Na página Gerenciamento de contas, selecione as contas para as quais você gostaria de ativar um tipo de verificação.
5. Escolha Ativar e selecione o tipo de verificação que você gostaria de ativar.
6. (Recomendado) Repita essas etapas em cada uma Região da AWS das quais você deseja ativar esse tipo de escaneamento.

API

Execute a operação Habilitar a API. Na solicitação, forneça os IDs de conta para os quais você está ativando as verificações, o token de idempotência e um ou mais dos `EC2`, `ECR`, `LAMBDA` ou `LAMBDA_CODE` para `resourceTypes`, para ativar as verificações desse tipo.

# Verificar as instâncias do Amazon EC2 com o Amazon Inspector

A verificação sem agente do Amazon Inspector para o Amazon EC2 está em versão prévia. O uso do recurso de verificação sem agente do Amazon EC2 está sujeito à Seção 2 dos Termos de serviço da AWS ("Betas e versões prévias").

A verificação do Amazon Inspector EC2 extrai metadados da instância do EC2 e, em seguida, compara esses metadados com regras coletadas de comunicados de segurança para produzir descobertas. O Amazon Inspector verifica instâncias em busca de vulnerabilidades de pacotes e problemas de acessibilidade de rede. Para obter informações sobre os tipos de descobertas produzidas para esses problemas, consulte Tipos de descoberta no Amazon Inspector.

O Amazon Inspector realiza verificações de acessibilidade de rede uma vez a cada 24 horas, enquanto as verificações de vulnerabilidade de pacotes são executadas em uma cadência variável, dependendo do método de verificação associado à instância.

Métodos de verificação

As verificações de vulnerabilidades de pacotes podem ser executadas usando um método de verificação baseado em agente ou sem agente. Esses métodos de verificação determinam como e quando o Amazon Inspector coleta o inventário de software de uma instância do EC2 para verificações de vulnerabilidades de pacotes. O método baseado em agente depende do agente SSM para coletar inventário de software, enquanto o método sem agente usa snapshots do Amazon EBS em vez de um agente.

Os métodos de verificação usados pelo Amazon Inspector dependem da configuração do modo de verificação da sua conta. Para obter mais informações, consulte Gerenciar o modo de digitalização.

Para ativar verificações do Amazon EC2, consulte Ativar um tipo de verificação.

# Verificação baseada em agente

As verificações baseadas em agente são executadas continuamente usando o agente SSM em todas as instâncias qualificadas. Para verificações baseadas em agente, o Amazon Inspector usa associações SSM e plug-ins instalados por meio dessas associações para coletar inventário de software de suas instâncias. Além das verificações de vulnerabilidades de pacotes de sistemas operacionais, a verificação baseada em agente do Amazon Inspector também pode detectar vulnerabilidades de pacotes de linguagens de programação de aplicativos em instâncias baseadas em Linux por meio de Inspeção detalhada do Amazon Inspector para instâncias do Amazon EC2 Linux.

O processo a seguir explica como o Amazon Inspector usa o SSM para coletar inventário e realizar verificações baseadas em agente:

1. O Amazon Inspector cria associações SSM na conta para coletar inventário de suas instâncias. Para alguns tipos de instância (Windows e Linux), essas associações instalam plug-ins em instâncias individuais para coletar inventário.
2. Usando o SSM, o Amazon Inspector extrai o inventário de pacotes de uma instância.
3. O Amazon Inspector avalia o inventário extraído e gera descobertas para as vulnerabilidades detectadas.

## Instâncias qualificadas

O Amazon Inspector usará o método baseado em agente para verificar uma instância se ela atender às seguintes condições:

- A instância tem um sistema operacional compatível. Para ver uma lista de sistemas operacionais compatíveis, consulte a coluna Suporte de verificação baseada em agente do the section called “Sistemas operacionais com suporte ao escaneamento do Amazon EC2”.
- A instância não é excluída das verificações pelas tags de exclusão do Amazon Inspector EC2.
- A instância é gerenciada pelo SSM. Para obter instruções sobre como verificar e configurar o agente, consulte Configurar o atendente do SSM.

## Comportamentos de verificação baseados em agente

Ao usar o método de verificação baseado em agente, o Amazon Inspector inicia novas verificações de vulnerabilidades de instâncias do EC2 nas seguintes situações:

- Ao executar uma nova instância do EC2.
- Ao instalar um novo software em uma instância do EC2 (Linux e Mac).
- Quando o Amazon Inspector adiciona um novo item de CVEs (vulnerabilidades e exposições comuns) ao seu banco de dados, e essa CVE é relevante para sua instância do EC2 (Linux e Mac).

O Amazon Inspector atualiza o campo Última verificação para uma instância do EC2 quando uma verificação inicial é concluída. Depois disso, o campo Última verificação é atualizado quando o Amazon Inspector avalia o inventário do SSM (a cada 30 minutos por padrão) ou quando uma instância é verificada novamente porque um novo CVE que afeta essa instância foi adicionado ao banco de dados do Amazon Inspector.

Você pode conferir quando uma instância do EC2 foi verificada pela última vez em busca de vulnerabilidades na guia Instâncias, na página Gerenciamento de contas, ou usando o comando ListCoverage.

## Configurar o atendente do SSM

Para que o Amazon Inspector detecte vulnerabilidades de software em uma instância do Amazon EC2 usando o método de verificação baseado em agente, a instância deve ser uma instância gerenciada no Amazon EC2 Systems Manager (SSM). Uma instância gerenciada do SSM tem o atendente do SSM instalado e em funcionamento, e o SSM tem permissão para gerenciar a instância. Se você já estiver usando o SSM para gerenciar suas instâncias, nenhuma outra etapa será necessária para verificações baseadas em agente.

O atendente de SSM é instalado por padrão em instâncias do EC2 criadas de algumas imagens de máquina da Amazon (AMIs). Para obter mais informações, consulte Sobre o atendente do SSM no Guia do usuário do AWS Systems Manager . No entanto, mesmo que esteja instalado, talvez seja necessário ativar o atendente do SSM manualmente e conceder permissão ao SSM para gerenciar sua instância.

O procedimento a seguir descreve como configurar uma instância do Amazon EC2 como uma instância gerenciada usando um perfil de instância do IAM. O procedimento também fornece links para informações mais detalhadas no Guia do usuário do AWS Systems Manager .

AmazonSSMManagedInstanceCore é a política recomendada a ser usada ao anexar um perfil de instância. Esta política tem todas as permissões necessárias para o escaneamento do EC2 do Amazon Inspector.

> **Note**
>
> Você também poderá automatizar o gerenciamento de SSM de todas as suas instâncias do EC2, sem o uso de perfis de instância do IAM usando a Configuração de gerenciamento de host padrão do SSM. Para obter mais informações, consulte Configuração de gerenciamento de host padrão.

Para configurar o SSM para uma instância do Amazon EC2

1. Se ele ainda não tiver sido instalado pelo fornecedor do sistema operacional, instale o atendente do SSM. Para obter mais informações, consulte Trabalhar com o atendente do SSM.
2. Use o AWS CLI para verificar se o agente SSM está em execução. Para obter mais informações, consulte Verificar o status do atendente do SSM e iniciar o atendente.
3. Conceda permissão para que o SSM gerencie sua instância. Conceda permissão criando um perfil de instância do IAM e anexando-o à sua instância. Recomendamos o uso da política AmazonSSMManagedInstanceCore, porque essa política tem as permissões para SSM Distributor, SSM Inventory e SSM State Manager, que o Amazon Inspector precisa para fazer verificações. Para obter instruções sobre como criar um perfil de instância com essas permissões e anexá-lo a uma instância, consulte Configurar permissões de instância para o Gerenciador de Sistemas.
4. (Opcional) Ative as atualizações automáticas para o atendente do SSM. Para obter mais informações, consulte Automatizar atualizações para o atendente do SSM.
5. (Opcional) Configure o Systems Manager para usar um endpoint Amazon Virtual Private Cloud (Amazon VPC). Para obter mais informações, consulte Criar o endpoint da VPC do Amazon.

> **Important**
>
> O Amazon Inspector exige uma associação do Gerenciador de Sistemas e do Gerenciador de Estado em sua conta para coletar o inventário de aplicativos de software. O Amazon Inspector cria automaticamente uma associação chamada `InspectorInventoryCollection-do-not-delete`, caso ainda não exista.
> O Amazon Inspector também exige uma sincronização de dados de recursos e cria automaticamente uma chamada `InspectorResourceDataSync-do-not-delete`, caso ainda não exista. Para obter mais informações, consulte Configurar a sincronização de dados de recursos para o Inventário no Guia do usuário do AWS Systems Manager . Cada conta

pode ter um número definido de sincronizações de dados de recursos por região. Para obter mais informações, consulte Número máximo de sincronizações de dados de recursos ( Conta da AWS por região) em endpoints e cotas do SSM. Se atingiu esse máximo, precisará excluir uma sincronização de dados de recursos, consulte Gerenciar de sincronizações de dados de recursos.

### Recursos do SSM criados para verificação

O Amazon Inspector requer vários recursos do SSM na conta para executar verificações do Amazon EC2. Os seguintes recursos são criados ao ativar o escaneamento do EC2 do Amazon Inspector pela primeira vez:

> **Note**
>
> Se algum desses recursos de SSM for excluído enquanto a verificação do Amazon Inspector Amazon EC2 estiver ativada para sua conta, o Amazon Inspector tentará recriá-los no próximo intervalo de verificação.

`InspectorInventoryCollection-do-not-delete`

Esta é uma associação do Gerenciador de Sistemas e do Gerenciador de Estado (SSM) que o Amazon Inspector usa para coletar inventário de aplicativos de software de suas instâncias do Amazon EC2. Se a sua conta já tiver uma associação do SSM para coletar inventário de `InstanceIds*`, o Amazon Inspector a usará em vez de criar a sua própria.

`InspectorResourceDataSync-do-not-delete`

Esta é uma sincronização de dados de recursos que o Amazon Inspector usa para enviar dados de inventário coletados de suas instâncias do Amazon EC2 para um bucket do Amazon S3 de propriedade do Amazon Inspector. Para obter mais informações, consulte Configurar a sincronização de dados de recursos para o Inventário no Guia do usuário do AWS Systems Manager .

`InspectorDistributor-do-not-delete`

Esta é uma associação do SSM que o Amazon Inspector usa para verificar as instâncias do Windows. Essa associação instala o plug-in do SSM do Amazon Inspector em suas instâncias do Windows. Se o arquivo do plug-in for excluído inadvertidamente, essa associação o reinstalará no próximo intervalo de associação.

`InvokeInspectorSsmPlugin-do-not-delete`

Esta é uma associação do SSM que o Amazon Inspector usa para verificar as instâncias do Windows. Essa associação permite que o Amazon Inspector inicie as verificações usando o plug-in. Você também poderá usá-lo para definir intervalos personalizados para as verificações de instâncias do Windows. Para ter mais informações, consulte Definir horários personalizados para verificações de instâncias do Windows.

`InspectorLinuxDistributor-do-not-delete`

Esta é uma associação SSM que o Amazon Inspector usa para a inspeção profunda do Amazon EC2 Linux. Essa associação instala o plug-in do SSM do Amazon Inspector nas instâncias do Linux.

`InvokeInspectorLinuxSsmPlugin-do-not-delete`

Esta é uma associação SSM que o Amazon Inspector usa para a inspeção profunda do Amazon EC2 Linux. Essa associação permite que o Amazon Inspector inicie as verificações usando o plug-in.

> **Note**
>
> Quando você desativa o Amazon Inspector, a digitalização ou a inspeção profunda do Amazon EC2, todos os recursos de SSM serão automaticamente desinstalados dos hosts Linux correspondentes.

## Verificação sem agente

O Amazon Inspector usa um método de verificação sem agente em instâncias qualificadas quando sua conta está no modo de verificação híbrida (que inclui escaneamentos baseados em agentes e sem agentes). No caso de verificações sem agente, o Amazon Inspector usa snapshots do EBS para coletar um inventário de software das suas instâncias. As instâncias verificadas usando o método sem agente são verificadas em busca de vulnerabilidades no pacote do sistema operacional e no pacote da linguagem de programação do aplicativo.

> **Note**
>
> Ao verificar instâncias do Linux em busca de vulnerabilidades de pacotes de linguagem de programação de aplicativos, o método sem agente verifica todos os caminhos disponíveis,

enquanto a verificação baseada em agente verifica apenas os caminhos padrão e caminhos adicionais especificados como parte do Inspeção detalhada do Amazon Inspector para instâncias do Amazon EC2 Linux. Isso pode fazer com que a mesma instância tenha descobertas diferentes, dependendo se ela for verificada usando o método baseado em agente ou o método sem agente.

O processo a seguir explica como o Amazon Inspector usa snapshots do EBS para coletar inventário e realizar verificações sem agente:

1. O Amazon Inspector cria um snapshot do EBS de todos os volumes anexados à instância. Enquanto o Amazon Inspector o estiver utilizando, o snapshot será armazenado na conta e marcado com o `InspectorScan` como chave de tag e um ID de digitalização exclusivo como valor de tag.
2. O Amazon Inspector recupera dados dos snapshots usando as APIs diretas do EBS e os avalia em busca de vulnerabilidades. As descobertas são geradas para todas as vulnerabilidades detectadas.
3. O Amazon Inspector exclui os snapshots do EBS criados na conta.

## Instâncias qualificadas

O Amazon Inspector usará o método sem agente para verificar uma instância se ela atender às seguintes condições:

- A instância tem um sistema operacional compatível. Para ver uma lista de sistemas operacionais compatíveis, consulte a coluna Suporte de verificação baseada em agente do the section called “Sistemas operacionais com suporte ao escaneamento do Amazon EC2”.
- A instância não é excluída das verificações pelas tags de exclusão do Amazon Inspector EC2.
- A instância tem um status de `Unmanaged EC2 instance`, `Stale inventory`, ou `No inventory`.
- A instância é respaldada por EBS e tem um dos seguintes formatos de sistema de arquivos:
  - `ext3`
  - `ext4`
  - `xfs`

### Comportamentos de verificação sem agente

Quando a conta está configurada para verificação híbrida, o Amazon Inspector realiza verificações sem agente em instâncias qualificadas a cada 24 horas. O Amazon Inspector detecta e verifica instâncias recém-qualificadas a cada hora, o que inclui novas instâncias sem agentes SSM ou instâncias pré-existentes com status que foram alterados para `SSM_UNMANAGED`.

O Amazon Inspector atualiza o campo Última verificação de uma instância do Amazon EC2 sempre que verifica snapshots extraídos de uma instância após uma verificação sem agente.

Você pode conferir quando uma instância do EC2 foi verificada pela última vez em busca de vulnerabilidades na guia Instâncias, na página Gerenciamento de contas, ou usando o comando ListCoverage.

## Gerenciar o modo de digitalização

O modo de verificação do EC2 determina quais métodos de verificação o Amazon Inspector usará ao realizar verificações do EC2 na conta. Você pode visualizar o modo de verificação da conta na página de configurações de verificação do EC2 em Configurações gerais. Contas independentes ou administradores delegados do Amazon Inspector podem alterar o modo de verificação. Quando você define o modo de verificação como administrador delegado do Amazon Inspector, esse modo de verificação é definido para todas as contas de membro da empresa. O Amazon Inspector tem os seguintes modos de verificação:

Verificação baseada em agente — Nesse modo de verificação, o Amazon Inspector usará exclusivamente o método de verificação baseado em agente ao verificar vulnerabilidades de pacotes. Este modo de verificação apenas verifica instâncias gerenciadas pelo SSM na conta, mas tem a vantagem de fornecer verificações contínuas em resposta a novos CVEs ou alterações nas instâncias. A verificação baseada em agente também fornece inspeção detalhada do Amazon Inspector para instâncias qualificadas. Este é o modo de verificação padrão para contas recém-ativadas.

Verificação híbrida — Nesse modo de verificação, o Amazon Inspector usa uma combinação de métodos baseados em agente e sem agente para verificar vulnerabilidades de pacotes. Para instâncias EC2 qualificadas que têm o agente SSM instalado e configurado, o Amazon Inspector usará o método baseado em agente. Para instâncias qualificadas que não são gerenciadas pelo SSM, o Amazon Inspector usará o método sem agente para instâncias qualificadas com suporte do EBS.

Para alterar o modo de digitalização

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região em que você deseja alterar o modo de digitalização do EC2.
3. No painel de navegação lateral, em Configurações gerais, selecione Configurações de escaneamento do EC2.
4. Em Modo de digitalização, selecione Editar.
5. Selecione um modo de verificação e selecione Salvar alterações.

## Excluir instâncias das verificações do Amazon Inspector

Marque determinadas instâncias para excluí-las das verificações do Amazon Inspector. Excluir instâncias das verificações pode ajudar a evitar alertas inacionáveis. Você não é cobrado pelas instâncias excluídas.

Para excluir uma instância do EC2 das verificações, marque essa instância com a seguinte chave:

- `InspectorEc2Exclusion`

O valor é opcional.

Para obter mais informações sobre como adicionar tags, consulte Marcar os recursos do Amazon EC2.

Além disso, você pode excluir um volume criptografado do EBS das verificações sem agente marcando a AWS KMS chave usada para criptografar esse volume com a tag. `InspectorEc2Exclusion` Para obter mais informações, consulte Marcação de chaves

## Sistemas operacionais compatíveis

O Amazon Inspector verifica as instâncias EC2 com suporte para Mac, Windows e Linux em busca de vulnerabilidades em pacotes do sistema operacional. Para instâncias do Linux, o Amazon Inspector pode produzir descobertas para pacotes de linguagens de programação de aplicativos usando Inspeção detalhada do Amazon Inspector para instâncias do Amazon EC2 Linux. Para instâncias do Mac e do Windows, somente pacotes do sistema operacional são verificados.

Para obter informações sobre os sistemas operacionais compatíveis, incluindo qual sistema operacional pode ser verificado sem um agente SSM, consulte Sistemas operacionais com suporte ao escaneamento do Amazon EC2.

## Inspeção detalhada do Amazon Inspector para instâncias do Amazon EC2 Linux

O Amazon Inspector expande sua cobertura de escaneamento do Amazon EC2 para incluir uma inspeção profunda. Com uma inspeção profunda, o Amazon Inspector detecta vulnerabilidades de pacotes de linguagens de programação de aplicativos em suas instâncias do Amazon EC2 baseadas em Linux.

O Amazon Inspector verifica os caminhos padrão para bibliotecas de pacotes de linguagens de programação. Você também pode configurar caminhos personalizados além dos caminhos padrão. Para ter mais informações, consulte Caminhos personalizados para a inspeção profunda do Amazon Inspector.

O Amazon Inspector realiza análises de inspeção aprofundadas usando dados coletados com o plug-in Amazon Inspector SSM. Para gerenciar o plug-in e realizar uma inspeção profunda para Linux, o Amazon Inspector cria automaticamente a seguinte associação SSM `InvokeInspectorLinuxSsmPlugin-do-not-delete` em sua conta. Isso ocorre quando o Amazon Inspector ativa a inspeção profunda.

O Amazon Inspector coleta inventário atualizado de aplicativos de instâncias para inspeção detalhada a cada 6 horas.

Para ver uma lista de linguagens de programação compatível com o Amazon Inspector para inspeção detalhada, consulte Linguagens de programação suportadas: inspeção profunda do Amazon EC2.

> **Note**
>
> A inspeção profunda não dá suporte às instâncias do Windows ou Mac.

## Ativar ou desativar a inspeção detalhada

> **Note**
>
> A inspeção profunda é ativada automaticamente como parte do escaneamento do Amazon EC2 para contas que ativam o Amazon Inspector após 17 de abril de 2023.

Você pode verificar se a inspeção detalhada está ativa para uma conta no console do Amazon Inspector na coluna de verificação do Amazon EC2 na página de Gerenciamento de contas. Se a inspeção detalhada não estiver ativa, esta coluna indicará Ativado (Inspeção detalhada desativada). Para verificar o status de ativação programaticamente, use a API GetEc2DeepInspectionConfiguration. Ou, para várias contas, use a API BatchGetMemberEc2DeepInspectionStatus.

Se você tiver ativado o Amazon Inspector antes de 17 de abril de 2023, poderá ativar a inspeção detalhada por meio do banner do console ou da API UpdateEc2DeepInspectionConfiguration. Se você for o administrador delegado de uma organização no Amazon Inspector, poderá usar a API BatchUpdateMemberEc2DeepInspectionStatus para ativar para você e as contas de membro.

Você pode desativar a inspeção detalhada por meio da API UpdateEc2DeepInspectionConfiguration. As contas de membros de uma organização não podem desativar a inspeção detalhada. Em vez disso, a conta de membro deve ser desativada pelo administrador delegado usando a API BatchUpdateMemberEc2DeepInspectionStatus.

## Sobre o plug-in do SSM do Amazon Inspector para Linux

O Amazon Inspector usa o plug-in Amazon Inspector SSM para realizar uma inspeção detalhada das instâncias do Linux. O plug-in do SSM do Amazon Inspector é instalado automaticamente nas instâncias do Linux no seguinte diretório: `/opt/aws/inspector/bin`. O nome do executável é `inspectorssmplugin`.

> **Note**
>
> O Amazon Inspector usa o distribuidor do Gerenciador de Sistemas para implantar o plug-in na instância do Amazon EC2. O distribuidor do Gerenciador de Sistemas oferece suporte aos sistemas operacionais listados como plataformas e arquiteturas de pacotes com suporte no guia do Gerenciador de Sistemas. O sistema operacional da sua instância do Amazon EC2

deve ser compatível com o Systems Manager Distributor e o Amazon Inspector para que o Amazon Inspector execute verificações de inspeção detalhadas.

O Amazon Inspector cria os seguintes diretórios de arquivos para gerenciar dados coletados para inspeção detalhada pelo plug-in SSM do Amazon Inspector:

- `/opt/aws/inspector/var/input`
- `/opt/aws/inspector/var/output`
  - Os `packages.txt` neste diretório armazenam os caminhos completos para os pacotes encontrados pela inspeção detalhada. Se o Amazon Inspector detectou o mesmo pacote várias vezes em sua instância, esse arquivo listará cada local em que o pacote foi encontrado.

O Amazon Inspector armazena os registros do plug-in no diretório `/var/log/amazon/inspector`.

Desinstalar o plug-in do SSM do Amazon Inspector

Se o arquivo `inspectorssmplugin` for excluído inadvertidamente, a associação de `InspectorLinuxDistributor-do-not-delete` do SSM de tentará reinstalar o plug-in no próximo intervalo de verificação.

Se você desativar o escaneamento do Amazon EC2, o plug-in será automaticamente desinstalado de todos os hosts Linux.

## Caminhos personalizados para a inspeção profunda do Amazon Inspector

Você pode configurar caminhos personalizados para que o Amazon Inspector pesquise quando ele executa uma inspeção profunda de suas instâncias Linux do Amazon EC2. Quando você adiciona um caminho personalizado, o Amazon Inspector verifica os pacotes nesse diretório e todos os subdiretórios dentro dele.

Todas as contas podem definir até 5 caminhos personalizados para suas contas individuais. Se você for o administrador delegado da sua organização, poderá definir cinco caminhos adicionais que se aplicarão a toda a organização. Isso equivale a um total de até 10 caminhos personalizados verificados por conta na organização.

O Amazon Inspector verifica todos os caminhos personalizados, além dos seguintes caminhos padrão que são verificados para todas as contas:

- `/usr/lib`

- `/usr/lib64`
- `/usr/local/lib`
- `/usr/local/lib64`

> **Note**
>
> Os caminhos personalizados devem ser caminhos locais. O Amazon Inspector não verifica os caminhos de rede mapeados, como montagens do NFS (Network File System) ou montagens do sistema de arquivos Amazon S3.

Formatação para caminhos personalizados

O exemplo a seguir é do formato de um caminho personalizado: `/home/usr1/project01`

Seus caminhos personalizados não podem exceder 256 caracteres.

Há um limite de 5.000 pacotes por instância e um limite máximo de tempo de coleta do inventário de pacotes de 15 minutos. É recomendável que você tente escolher caminhos personalizados para ajudar a evitar esses limites.

Definir um caminho personalizado no console

Console

Faça login como administrador delegado do Amazon Inspector e siga as etapas a seguir para adicionar caminhos personalizados para sua organização.

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região em que você deseja ativar a digitalização padrão Lambda.
3. No painel de navegação lateral, em Configurações gerais, selecione Configurações de escaneamento do EC2.
4. Em Caminhos personalizados para sua própria conta, selecione Editar para adicionar caminhos à sua conta individual. Se você for o administrador delegado, poderá escolher Editar no painel Caminhos personalizados para sua organização para adicionar caminhos personalizados para todas as contas dentro da organização.

5. Insira seus caminhos personalizados nas caixas de texto.
6. Escolha Salvar para salvar seus caminhos personalizados. O Amazon Inspector incluirá esses caminhos em sua próxima inspeção profunda.

API

Execute o comando UpdateEc2DeepInspectionConfiguration. Para especificar os `packagePaths` uma matriz de caminhos a serem verificados.

Linguagens de programação compatíveis

Para instâncias Linux, a inspeção detalhada do Amazon Inspector pode produzir descobertas para pacotes de linguagem de programação de aplicativos, além de vulnerabilidades em pacotes de sistema operacional. Para instâncias do Mac e do Windows, somente pacotes do sistema operacional são verificados.

Para obter informações sobre as linguagens de programação compatíveis, consulte Linguagens de programação suportadas para a inspeção profunda do Amazon Inspector.

## Verificação das instâncias do EC2 do Windows com o Amazon Inspector

> **Note**
>
> Em 31 de agosto de 2022, o Amazon Inspector expandiu sua cobertura de escaneamento do Amazon EC2 para incluir instâncias EC2 em execução no Windows.

O Amazon Inspector descobre automaticamente todas as instâncias com suporte do Windows e as inclui na verificação contínua sem nenhuma ação extra. Para obter informações sobre quais instâncias têm suporte, consulte Sistemas operacionais com suporte ao escaneamento do Amazon EC2.

Ao contrário das verificações para instâncias baseadas em Linux, o Amazon Inspector executa no Windows verificações em intervalos regulares. As instâncias do Windows são inicialmente verificadas na descoberta e depois verificadas a cada 6 horas. No entanto, o intervalo padrão de verificação de 6 horas é ajustável. Para ter mais informações, consulte Definir horários personalizados para verificações de instâncias do Windows. A seguir está uma visão geral de como o Amazon Inspector verifica as instâncias do Windows:

1. Quando o escaneamento do Amazon EC2 é ativado, o Amazon Inspector cria novas associações de SSM para os recursos do Windows: `InspectorDistributor-do-not-delete`, `InspectorInventoryCollection-do-not-delete` e `InvokeInspectorSsmPlugin-do-not-delete`.
2. A associação `InspectorDistributor-do-not-delete` SSM usa o documento `AWS-ConfigureAWSPackage` SSM e o pacote `AmazonInspector2-InspectorSsmPlugin` SSM Distributor para instalar o plug-in Amazon Inspector SSM em suas instâncias. Windows Consulte Sobre o plug-in Amazon Inspector SSM para Windows Para mais informações.
3. A associação `InvokeInspectorSsmPlugin-do-not-delete` SSM executa o plug-in Amazon Inspector SSM em intervalos regulares para coletar dados da instância e gerar descobertas do Amazon Inspector. Por padrão, o intervalo é a cada 6 horas. No entanto, você poderá personalizar isso definindo uma expressão cron ou uma expressão rate para a associação usando o SSM. Para obter mais informações, consulte Referência: expressão cron e expressão rate para Gerenciador de Sistemas no Guia do usuário do AWS Systems Manager .

> **Note**
>
> O Amazon Inspector envia arquivos de definição de OVAL (Linguagem Aberta de Determinação de Vulnerabilidade) atualizados para o bucket S3 em `inspector2-oval-prod-REGION`. Esse bucket do S3 contém as definições de OVAL usadas em verificações e não deve ser modificado. Alterar essa configuração impedirá que o Amazon Inspector verifique novas CVEs à medida que forem lançados.

## Requisitos de verificação do Amazon Inspector para instâncias do Windows

Para verificar uma instância do Windows, o Amazon Inspector exige que a instância atenda aos seguintes critérios:

- A instância é uma instância gerenciada por SSM. Para obter instruções sobre como configurar sua instância para verificação, consulte Configurar o atendente do SSM.
- O sistema operacional da instância é um dos sistemas operacionais com suporte pelo Windows. Para obter uma lista completa de sistemas operacionais com suporte, consulte Sistemas operacionais com suporte ao escaneamento do Amazon EC2.

- A instância tem o plug-in Amazon Inspector SSM instalado. O Amazon Inspector instala automaticamente o plug-in Amazon Inspector SSM para instâncias gerenciadas após a descoberta. Consulte o próximo tópico para obter detalhes sobre o plug-in.

> **Note**
>
> Se seu host estiver sendo executado em um Amazon VPC sem acesso de saída à Internet, a verificação do Windows exige que seu host consiga acessar endpoints regionais do Amazon S3. Para saber como configurar um endpoint da Amazon VPC do Amazon S3, consulte Criar um endpoint de gateway no Guia do usuário da Amazon Virtual Private Cloud. Se a sua política de endpoint do Amazon VPC está restringindo o acesso a buckets S3 externos, você deve permitir especificamente o acesso ao bucket mantido pelo Amazon Inspector no seu Região da AWS que armazena as definições OVAL usadas para avaliar sua instância. Este bucket tem o seguinte formato: `inspector2-oval-prod-REGION`.

## Sobre o plug-in Amazon Inspector SSM para Windows

O plug-in Amazon Inspector SSM é necessário para que o Amazon Inspector escaneie suas instâncias. Windows O plug-in Amazon Inspector SSM é instalado automaticamente em suas Windows instâncias em`C:\Program Files\Amazon\Inspector`, e o arquivo binário executável é nomeado. `InspectorSsmPlugin.exe`

Os seguintes locais de arquivo são criados para armazenar dados que o plug-in Amazon Inspector SSM coleta:

- `C:\ProgramData\Amazon\Inspector\Input`
- `C:\ProgramData\Amazon\Inspector\Output`
- `C:\ProgramData\Amazon\Inspector\Logs`

> **Note**
>
> Por padrão, o plug-in Amazon Inspector SSM é executado abaixo da prioridade normal.

### Desinstalar o plug-in do SSM do Amazon Inspector

Se o arquivo `InspectorSsmPlugin.exe` for excluído inadvertidamente, a associação de `InspectorDistributor-do-not-delete` do SSM reinstalará o plug-in no próximo intervalo de verificação do Windows. Se você quiser desinstalar o plug-in Amazon Inspector SSM, você pode usar a ação Desinstalar no documento. `AmazonInspector2-ConfigureInspectorSsmPlugin`

Além disso, o plug-in Amazon Inspector SSM será automaticamente desinstalado de todos os Windows hosts se você desativar o escaneamento do Amazon EC2.

> **Note**
>
> Se você desinstalar o Agente SSM antes de desativar o Amazon Inspector, o plug-in SSM do Amazon Inspector permanecerá no Windows host, mas não enviará mais dados para o plug-in SSM do Amazon Inspector. Para ter mais informações, consulte Desativar o Amazon Inspector.

## Definir horários personalizados para verificações de instâncias do Windows

Personalize o tempo entre as verificações das instância do Amazon EC2 do Windows, definindo uma expressão cron ou uma expressão rate para a associação de `InvokeInspectorSsmPlugin-do-not-delete` usando o SSM. Para obter mais informações, consulte Referência: expressão cron e expressão rate para Gerenciador de Sistemas no Guia do usuário do AWS Systems Manager ou use as instruções a seguir.

Selecione um dos exemplos de código a seguir para alterar a cadência de verificação das instâncias do Windows das 6 horas padrão para 12 horas usando uma expressão rate ou uma expressão cron.

Os exemplos a seguir exigem que você use o AssociationIdpara a associação chamada`InvokeInspectorSsmPlugin-do-not-delete`. Você pode recuperar seu AssociationIdexecutando o seguinte AWS CLI comando:

```
$ aws ssm list-associations --association-filter-list
 "key=AssociationName,value=InvokeInspectorSsmPlugin-do-not-delete" --region us-east-1
```

> **Note**
>
> AssociationIdÉ regional, então você precisa primeiro recuperar uma ID exclusiva para cada Região da AWS um. Em seguida, execute o comando para alterar a cadência de

verificação em cada região a ser definida um cronograma de verificação personalizado para as instâncias do Windows.

Example rate expression

```
$ aws ssm update-association \
--association-id "YourAssociationId" \
--association-name "InvokeInspectorSsmPlugin-do-not-delete" \
--schedule-expression "rate(12 hours)"
```

Example cron expression

```
$ aws ssm update-association \
--association-id "YourAssociationId" \
--association-name "InvokeInspectorSsmPlugin-do-not-delete" \
--schedule-expression "cron(0 0/12 * * ? *)"
```

# Verificar imagens de contêineres do Amazon ECR com o Amazon Inspector

O Amazon Inspector verifica imagens de contêineres armazenadas no Amazon ECR em busca de vulnerabilidades de software para gerar descobertas de Vulnerabilidade de pacote. Para obter informações sobre os tipos de descobertas produzidas para esses problemas, consulte Tipos de descoberta no Amazon Inspector.

Ao ativar as verificações do Amazon Inspector para o Amazon ECR, você define o Amazon Inspector como seu serviço de verificação preferido para seu registro privado. Isso substitui o escaneamento básico padrão, que é fornecido gratuitamente pelo Amazon ECR, pelo Escaneamento avançado, que é fornecido e cobrado pelo Amazon Inspector.

O escaneamento avançado fornecido pelo Amazon Inspector oferece o benefício da verificação de vulnerabilidades para pacotes de sistemas operacionais e linguagens de programação no nível do registro. Analise as descobertas usando o escaneamento avançado no nível da imagem, para cada camada da imagem, no console do Amazon ECR. Além disso, você pode analisar e trabalhar com essas descobertas em outros serviços não disponíveis para descobertas básicas de escaneamento, incluindo AWS Security Hub a Amazon EventBridge. Você pode ver as descobertas descobertas por

escaneamentos no console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home. Para obter informações sobre como trabalhar com descobertas, consulte Gerenciar descobertas no Amazon Inspector.

Para obter instruções sobre como ativar as verificações do Amazon ECR, consulte. Ativar um tipo de verificação

## Comportamentos de verificação para o escaneamento do Amazon ECR

Quando você ativa o escaneamento ECR pela primeira vez e seu repositório é configurado para digitalização contínua, o Amazon Inspector detecta todas as imagens elegíveis que você enviou em 30 dias ou retirou nos últimos 90 dias. Em seguida, o Amazon Inspector escaneia as imagens detectadas e define seu status de digitalização como. `active` O Amazon Inspector continua monitorando imagens desde que elas tenham sido enviadas ou retiradas nos últimos 90 dias (por padrão) ou dentro da duração de redigitalização do ECR que você configura. Para ter mais informações, consulte Configurando a duração da nova digitalização do ECR.

Para a varredura contínua, o Amazon Inspector inicia novas análises de vulnerabilidade de imagens de contêineres nas seguintes situações:

- Sempre que uma nova imagem de contêiner é enviada.
- Sempre que o Amazon Inspector adiciona um novo item de CVEs (vulnerabilidades e exposições comuns) ao seu banco de dados, e esse CVE é relevante para a imagem do contêiner (somente verificação contínua).

Se você configurar seu repositório para digitalização por push, as imagens serão digitalizadas somente quando você as enviar por push.

Na guia Imagens de contêiner na página de Gerenciamento de contas ou usando a API ListCoverage, você pode verificar quando uma imagem de contêiner foi verificada pela última vez em busca de vulnerabilidades. O Amazon Inspector atualiza o campo Última verificação em de uma imagem do Amazon ECR em resposta aos seguintes eventos:

- Quando o Amazon Inspector conclui uma verificação inicial de uma imagem de contêiner.
- Quando o Amazon Inspector verifica novamente uma imagem de contêiner porque um novo item de CVEs (vulnerabilidades e exposições comuns) que afeta essa imagem de contêiner foi adicionado ao banco de dados do Amazon Inspector.

## Sistemas operacionais e tipos de mídia com suporte

Para obter informações sobre os sistemas operacionais com suporte, consulte Sistemas operacionais com suporte ao escaneamento do Amazon ECR.

As verificações do Amazon Inspector dos repositórios do Amazon ECR abrangem os seguintes tipos de mídia com suporte:

- `"application/vnd.docker.distribution.manifest.v1+json"`
- `"application/vnd.docker.distribution.manifest.v1+prettyjws"`
- `"application/vnd.oci.image.manifest.v1+json"`
- `"application/vnd.docker.distribution.manifest.v2+json"`

> **Note**
>
> Não há suporte para imagens `DockerV2ListMediaType` e imagens de rascunho.

## Configurar o escaneamento avançado para repositórios do Amazon ECR

Ao ativar as verificações do Amazon Inspector para imagens de contêineres do Amazon ECR, você altera a configuração de verificação do seu registro privado. O tipo de escaneamento do registro foi alterado de Escaneamento básico para Escaneamento avançado, fornecido pelo Amazon Inspector. Para obter mais informações, consulte Verificação de imagens no guia do usuário do Amazon ECR.

Gerencie as configurações para o escaneamento avançado no nível do repositório no ECR. Você pode escolher a verificação contínua ou a verificação por push para seus repositórios. A verificação contínua inclui verificações imediatas e novas verificações automatizadas. A verificação sob pressão verifica somente ao enviar uma imagem pela primeira vez. Para ambas as opções, você pode refinar o escopo da verificação por meio de filtros de inclusão. Por padrão, ao ativar o escaneamento avançado pela primeira vez, suas configurações são definidas para Verificar continuamente todos os repositórios.

Para definir suas configurações de escaneamento avançado

1. Abra o console do Amazon ECR em https://console.aws.amazon.com/ecr/
2. No Região da AWS seletor no canto superior direito da página, selecione a região que tem os repositórios que você está digitalizando.

3. No painel de navegação, escolha Registro privado e selecione Verificação.
4. Em Tipo de verificação, verifique se a opção Escaneamento avançado está selecionado. Se não estiver, selecione Escaneamento avançado.

   Por padrão, a opção Verificar continuamente todos os repositórios é selecionada, o que ativa a cobertura completa de verificação do Amazon Inspector para todos os repositórios.
5. Desmarque a opção Verificar continuamente todos os repositórios para filtrar quais repositórios são verificados continuamente ou por push.

Para obter mais informações sobre a configuração de escaneamentos avançados, consulte Usar o escaneamento avançado no guia do usuário do Amazon ECR.

## Configurando a duração da nova digitalização do ECR

A configuração de duração da nova verificação do ECR determina por quanto tempo o Amazon Inspector monitora continuamente as imagens dos contêineres nos repositórios. Você pode configurar a duração da nova digitalização para a data de envio da imagem e a data de extração da imagem. A duração padrão da verificação para novas contas, incluindo novas contas adicionadas a uma organização, é de 90 dias.

Duração da data de envio da imagem

A duração da data de envio da imagem determina por quanto tempo o Amazon Inspector monitora continuamente as imagens após elas serem enviadas aos repositórios após a data de extração mais recente. As seguintes opções estão disponíveis como durações de nova digitalização:

- 14 dias
- 30 dias
- 60 dias
- 90 dias (padrão)
- 180 dias
- Tempo de vida

Duração da data de extração da imagem

A duração da data de extração da imagem determina por quanto tempo o Amazon Inspector monitora continuamente as imagens após a última data de extração. As seguintes opções estão disponíveis como durações de nova digitalização:

- 14 dias
- 30 dias
- 60 dias
- 90 dias (padrão)
- 180 dias

O Amazon Inspector continuará monitorando e digitalizando novamente uma imagem, desde que ela tenha sido enviada ou retirada dentro das datas de envio e extração configuradas. Se a imagem não tiver sido enviada ou retirada dentro das datas de envio e extração configuradas, o Amazon Inspector interromperá o monitoramento.

> **Note**
>
> Quando o Amazon Inspector para de monitorar uma imagem, ele define o código de status da digitalização da imagem como `inactive` e o código do motivo como. `expired` Em seguida, ele agenda todas as descobertas de imagens associadas para serem fechadas.

Defina a duração da nova verificação para melhor se adequar ao seu ambiente. Por exemplo, se você cria imagens com frequência, escolha uma duração de digitalização mais curta. Da mesma forma, se você usar imagens por longos períodos de tempo, escolha uma duração de digitalização maior.

Quando você configura a duração da nova verificação a partir de uma conta de administrador delegado, o Amazon Inspector aplica a configuração a todas as contas membros da organização.

Para configurar a duração da nova digitalização do ECR

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. No painel de navegação, escolha Configurações gerais e, em seguida, escolha Configurações de digitalização ECR.

3. Nas configurações de digitalização ECR, em Duração da nova digitalização ECR, escolha a duração da data de envio da imagem e a duração da data de extração da imagem que você deseja definir.
4. Selecione Save (Salvar). Suas novas configurações são aplicadas imediatamente.

> **Note**
>
> Se você aumentar a duração da data de envio, o Amazon Inspector aplicará a alteração a todas as imagens digitalizadas ativamente em repositórios configurados para digitalização contínua. No entanto, as imagens inativas permanecem inativas, mesmo que você as tenha enviado dentro da nova duração.

# AWS Lambda Funções de digitalização com o Amazon Inspector

O suporte do Amazon Inspector para AWS Lambda funções fornece avaliações de vulnerabilidade de segurança contínuas e automatizadas para funções e camadas do Lambda. O Amazon Inspector oferece dois tipos de verificação para Lambda. Esses tipos de verificação procuram diferentes tipos de vulnerabilidades.

Escaneamento padrão do Lambda do Amazon Inspector

Esse é o tipo padrão de escaneamento do Lambda. O escaneamento padrão do Lambda verifica as dependências do aplicativo dentro de uma função do Lambda e suas camadas em busca de vulnerabilidades de pacotes. Para ter mais informações, consulte Escaneamento padrão do Lambda.

Escaneamento de código do Lambda do Amazon Inspector

Esse tipo de escaneamento verifica o código do aplicativo personalizado em suas funções e camadas em busca de vulnerabilidades de código. Ative o escaneamento padrão do Lambda ou ative o escaneamento padrão do Lambda junto com o escaneamento de código do Lambda. Para ter mais informações, consulte Escaneamento de código do Lambda do Amazon Inspector.

Quando você ativa o escaneamento Lambda, o Amazon Inspector cria os AWS CloudTrail seguintes canais vinculados ao serviço em sua conta:

- `cloudtrail:CreateServiceLinkedChannel`

- `cloudtrail:DeleteServiceLinkedChannel`

O Amazon Inspector gerencia esses canais e os usa para monitorar seus CloudTrail eventos em busca de escaneamentos. Para obter mais informações sobre canais vinculados a serviços, consulte Visualização de canais vinculados a serviços CloudTrail usando a CLI. AWS

> **Note**
>
> Os canais vinculados ao serviço criados pelo Amazon Inspector permitem que você CloudTrail veja eventos em sua conta como se tivesse CloudTrail uma trilha, no entanto, recomendamos que você crie sua CloudTrail própria para gerenciar eventos em sua conta.

Para obter instruções sobre como ativar os escaneamentos da função do Lambda, consulte Ativar um tipo de verificação.

## Comportamentos de verificação para escaneamento de funções do Lambda

Após a ativação, o Amazon Inspector verifica todas as funções do Lambda invocadas ou atualizadas nos últimos 90 dias em sua conta. O Amazon Inspector inicia verificações de vulnerabilidade das funções do Lambda nas seguintes situações:

- Assim que o Amazon Inspector descobrir uma função do Lambda existente.
- Ao implantar uma nova função do Lambda no serviço do Lambda.
- Ao implantar uma atualização no código do aplicativo ou nas dependências de uma função do Lambda existente ou de suas camadas.
- Sempre que o Amazon Inspector adiciona um novo item de CVEs (vulnerabilidades e exposições comuns) ao seu banco de dados, e esse CVE é relevante para sua função.

O Amazon Inspector monitora cada função do Lambda ao longo de sua vida útil até que ela seja apagada ou excluída da verificação.

Na guia Funções do Lambda na página Gerenciamento de contas ou usando a API ListCoverage, você pode verificar quando uma função do Lambda foi verificada pela última vez em busca de vulnerabilidades. O Amazon Inspector atualiza o campo Última verificação em para uma função do Lambda em resposta aos seguintes eventos:

- Quando o Amazon Inspector conclui uma verificação inicial de uma função do Lambda.
- Quando uma função do Lambda é atualizada.
- Quando o Amazon Inspector verifica novamente uma função do Lambda porque um novo item de CVE que afeta essa função foi adicionado ao banco de dados do Amazon Inspector.

## Runtime com suporte e funções elegíveis

O Amazon Inspector suporta diferentes runtime para escaneamento padrão do Lambda e escaneamento de código do Lambda. Para obter uma lista dos tempos de execução com suporte para cada tipo de escaneamento, consulte Runtime com suporte: ao escaneamento padrão do Lambda do Amazon Inspector e Runtime com suporte: ao escaneamento de código do Lambda do Amazon Inspector.

Além de ter um runtime com suporte, uma função do Lambda precisa atender aos seguintes critérios para ser elegível para as verificações do Amazon Inspector:

- A função foi invocada ou atualizada nos últimos 90 dias.
- A função está marcada `$LATEST`.
- A função não é excluída das verificações por tags.

> **Note**
>
> As funções do Lambda que não foram invocadas ou modificadas nos últimos 90 dias são automaticamente excluídas das verificações. O Amazon Inspector retomará a verificação de uma função excluída automaticamente se ela for invocada novamente ou se forem feitas alterações no código da função do Lambda.

## Escaneamento padrão do Lambda do Amazon Inspector

A verificação padrão do Lambda do Amazon Inspector identifica vulnerabilidades de software nas dependências do pacote de aplicativos adicionadas ao código e nas camadas da função do Lambda. Por exemplo, se sua função do Lambda usa uma versão do pacote de `python-jwt` com uma vulnerabilidade conhecida, o escaneamento padrão do Lambda gerará uma descoberta para essa função.

Se o Amazon Inspector detectar uma vulnerabilidade nas dependências do pacote do aplicativo da função do Lambda, o Amazon Inspector produzirá uma descoberta detalhada do tipo de Vulnerabilidade do pacote.

Para obter instruções sobre como ativar um tipo de escaneamento, consulte Ativar um tipo de verificação.

> **Note**
>
> O escaneamento padrão do Lambda não verifica a dependência do AWS SDK instalada por padrão no ambiente de execução do Lambda. O Amazon Inspector verifica apenas dependências carregadas com o código de função ou herdadas de uma camada.

> **Note**
>
> Desativar o escaneamento padrão do Lambda do Amazon Inspector também desativará o escaneamento de código do Lambda do Amazon Inspector.

## Excluir as funções do escaneamento padrão do Lambda

Marque determinadas funções para excluí-las dos escaneamentos padrão do Lambda do Amazon Inspector. A exclusão de funções dos escaneamentos pode ajudar a evitar alertas inacionáveis.

Para excluir uma função do Lambda do escaneamento padrão do Lambda, marque a função com o seguinte par de valores-chave:

- Chave:`InspectorExclusion`
- Valor:`LambdaStandardScanning`

Para excluir uma função do escaneamento padrão do Lambda

1. Abra o console do Lambda em https://console.aws.amazon.com/lambda/.
2. Selecione a opção Funções.
3. Na tabela de funções, selecione o nome de uma função que você gostaria de excluir do escaneamento padrão do Lambda do Amazon Inspector.
4. Selecione Configuração e escolha Tags no menu.

5. Selecione Gerenciar tags e depois Adicionar nova tag.
6. No campo Chave, insira `InspectorExclusion` e, em seguida, no campo Valor, insira `LambdaStandardScanning`.
7. Selecione Salvar para adicionar a tag e excluir sua função do escaneamento padrão do Lambda do Amazon Inspector.

Para obter mais informações sobre como adicionar tags no Lambda, consulte Usar tags nas funções do Lambda.

## Escaneamento de código do Lambda do Amazon Inspector

> **Important**
>
> Escaneamento de código captura trechos de código das funções do Lambda para destacar as vulnerabilidades detectadas. Esses trechos podem mostrar credenciais codificadas ou outros materiais confidenciais em texto simples.

O escaneamento de código do Amazon Inspector Lambda escaneia o código do aplicativo personalizado dentro de uma função Lambda em busca de vulnerabilidades de código com base nas melhores práticas de segurança. AWS O escaneamento de código do Lambda pode detectar falhas de injeção, vazamentos de dados, criptografia fraca ou criptografia ausente em seu código. Para obter informações sobre as regiões disponíveis, consulte Disponibilidade de recursos específicos da região.

O escaneamento padrão do Lambda é um recurso que avalia as dependências do pacote de aplicativos usadas em uma função para CVEs (vulnerabilidades e exposições comuns). Ative o escaneamento de código do Lambda junto com o escaneamento padrão do Lambda.

O Amazon Inspector avalia o código do seu aplicativo de função do Lambda usando raciocínio automatizado e machine learning que analisa o código do seu aplicativo para uma conformidade geral de segurança. Ele identifica violações de políticas e vulnerabilidades com base em detectores internos desenvolvidos em colaboração com a Amazon. CodeGuru Para obter uma lista de possíveis detecções, consulte a Biblioteca de CodeGuru Detectores.

Se o Amazon Inspector detectar uma vulnerabilidade no código do aplicativo da função do Lambda, o Amazon Inspector produzirá uma descoberta detalhada do tipo de Vulnerabilidade de código. Esse

tipo de descoberta inclui a localização exata do problema no código, um trecho de código mostrando o problema e sugestões de correção. A correção sugerida inclui blocos de plug-and-play código que você pode usar para substituir suas linhas de código vulneráveis. Essas correções de código sugeridas são fornecidas além das orientações gerais de correção de código para essa descoberta.

> **Important**
>
> Como as sugestões de correção de código são possibilitadas por raciocínio automatizado e IA generativa, elas podem não funcionar conforme o esperado. Você é responsável pelas sugestões de correção de código que adota. Sempre analise as sugestões de correção de código antes de adotá-las. Talvez seja necessário fazer edições nas sugestões de correção de código para garantir que o código tenha o desempenho esperado. Consulte a Política de IA responsável.

## Criptografar seu código em descobertas de vulnerabilidade de código

Os trechos de código detectados em conexão com uma descoberta de vulnerabilidade de código usando a digitalização de código Lambda são armazenados pelo serviço. CodeGuru Por padrão, uma AWS chave própria controlada por CodeGuru é usada para criptografar seu código, no entanto, você pode usar sua própria chave gerenciada pelo cliente para criptografia por meio da API do Amazon Inspector. Para obter mais informações, consulte Criptografia em repouso para código em suas descobertas

O escaneamento de código do Lambda pode ser ativado junto com o escaneamento padrão do Lambda. Para obter instruções sobre como ativar um tipo de verificação, consulte Ativar um tipo de verificação.

## Excluir funções do escaneamento de código do Lambda

Marque determinadas funções para excluí-las dos escaneamentos de código do Lambda do Amazon Inspector. A exclusão de funções dos escaneamentos pode ajudar a evitar alertas inacionáveis.

Para excluir uma função do Lambda do Amazon Inspector, os escaneamentos de código do Lambda marcam a função com o seguinte par de valores-chave:

- Chave:`InspectorCodeExclusion`
- Valor:`LambdaCodeScanning`

Para excluir uma função do escaneamento de código do Lambda

1. Faça login no console do Lambda em https://console.aws.amazon.com/lambda/.
2. Selecione Funções.
3. Na tabela de funções, selecione o nome de uma função que você gostaria de excluir da escaneamento de código do Lambda do Amazon Inspector.
4. Selecione Configuração e escolha Tags no menu.
5. Selecione Gerenciar tags e depois Adicionar nova tag.
6. No campo Chave, insira `InspectorCodeExclusion` e, em seguida, no campo Valor, insira `LambdaCodeScanning`.
7. Selecione Salvar para adicionar a tag e excluir sua função do escaneamento de código do Lambda do Amazon Inspector.

Para obter mais informações sobre como adicionar tags no Lambda, consulte Usar tags nas funções do Lambda.

# Desativar um tipo de escaneamento

Desative um novo tipo de escaneamento do Amazon Inspector a qualquer momento. Ao desativar um tipo de escaneamento, você perde o acesso a todas as descobertas existentes que foram produzidas por esse tipo de escaneamento. Se você reativar o tipo de escaneamento, seus recursos elegíveis serão verificados e o Amazon Inspector produzirá novas descobertas. Para manter um registro dos dados de suas descobertas, exporte suas descobertas antes de desativar. Para ter mais informações, consulte Exportação de relatórios de descobertas do Amazon Inspector.

Quando você desativa um tipo de escaneamento, certas alterações podem ocorrer nessa AWS conta, dependendo do tipo de escaneamento que está sendo desativado. A seguir estão as alterações que ocorrerão ao desativar esses tipos de escaneamento:

- Escaneamento do Amazon EC2: ao desativar o escaneamento do Amazon EC2 do Amazon Inspector para uma conta, as seguintes associações de SSM usadas pelo Amazon Inspector são excluídas:
  - `InspectorDistributor-do-not-delete`
  - `InspectorInventoryCollection-do-not-delete`
  - `InspectorLinuxDistributor-do-not-delete`

  - `InvokeInspectorLinuxSsmPlugin-do-not-delete`
  - `InvokeInspectorSsmPlugin-do-not-delete`. Além disso, o plug-in Amazon Inspector SSM instalado por meio dessa associação é removido de todos os seus hosts. Windows Para ter mais informações, consulte Verificação das instâncias do Windows..
- Escaneamento do Amazon ECR: ao desativar a verificação de imagens de contêineres do Amazon ECR para uma conta, o tipo de escaneamento do Amazon ECR para essa conta muda de Escaneamento avançado com o Amazon Inspector para Escaneamento Básico com o Amazon ECR.
- Escaneamento padrão do Lambda: ao desativar o escaneamento padrão do Lambda em uma conta, ele desativa o escaneamento de código do Lambda se o escaneamento de código também estiver ativo. Além disso, o canal vinculado ao CloudTrail serviço criado quando a digitalização foi ativada é excluído.

## Desativar as verificações

A desativação de todos os tipos de escaneamento de uma conta desativa o Amazon Inspector dessa conta da Região da AWS. Para ter mais informações, consulte Desativar o Amazon Inspector.

Para concluir este procedimento para um ambiente com várias contas, siga estas etapas enquanto estiver conectado como administrador delegado do Amazon Inspector.

Console

Para desativar as verificações

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região em que você deseja desativar as digitalizações.
3. No painel de navegação, escolha Gerenciamento de contas.
4. Escolha a guia Contas para mostrar o status de verificação de uma conta.
5. Marque a caixa de seleção de cada conta a ser desativada as verificações.
6. Escolha Ações e, nas opções Desativar, selecione o tipo de verificação que você deseja desativar.
7. (Recomendado) Repita essas etapas em cada uma Região da AWS das quais você deseja desativar esse tipo de escaneamento.

### API

Execute a operação Desativar da API. Na solicitação, forneça os IDs da conta para os quais você está desativando as verificações e forneça `resourceTypes` um ou mais dos `EC2`, `ECR`, `LAMBDA` ou `LAMBDA_CODE` para desativar as verificações.

# O Center for Internet Security (CIS) verifica instâncias do EC2

Quando você habilita o escaneamento EC2 do Amazon Inspector para uma conta, você permite que o Amazon Inspector execute ou agende escaneamentos CIS. Os escaneamentos do Amazon Inspector CIS comparam os sistemas operacionais de suas instâncias do Amazon EC2 para ver se eles estão configurados de acordo com as recomendações de melhores práticas estabelecidas pelo Center for Internet Security. O programa CIS Security Benchmarks fornece linhas de base de configuração padrão do setor e melhores práticas para configurar um sistema com segurança. Para obter mais informações, consulte O que são benchmarks do CIS?

O Amazon Inspector executa escaneamentos CIS em instâncias de destino do Amazon EC2 com base nas tags de instância e no cronograma de escaneamento que você define em uma configuração de escaneamento. Para cada instância alvo, o Amazon Inspector executa uma série de verificações na instância. Cada verificação avalia se a configuração do sistema atende a uma recomendação específica do CIS Benchmark. Cada verificação tem um ID e um título de verificação do CIS, que se correlacionam diretamente com uma recomendação do CIS Benchmark para essa plataforma. Quando uma verificação é concluída, você pode ver os resultados e ver quais verificações sua instância passou, falhou ou ignorou para esse sistema.

## Requisitos de instância EC2 para escaneamentos do Amazon Inspector CIS

Para executar uma verificação CIS em sua instância, o Amazon Inspector exige que a instância atenda aos seguintes critérios:

- O sistema operacional da instância é um dos sistemas operacionais compatíveis com escaneamentos do CIS. Para obter uma lista completa de sistemas operacionais com suporte, consulte Sistemas operacionais suportados: digitalização CIS.
- A instância é uma instância gerenciada pelo Amazon EC2 Systems Manager (SSM). Para obter mais informações, consulte Trabalhar com o atendente do SSM.
- A instância tem o plug-in Amazon Inspector SSM instalado. O Amazon Inspector instala automaticamente esse plug-in para instâncias gerenciadas por SSM.
- A instância tem um perfil de instância que concede permissões ao SSM para gerenciar a instância e ao Amazon Inspector para executar escaneamentos do CIS para essa instância. Para

conceder essas permissões, anexe as ManagedCispolicy políticas AmazonInspector2FullAccess, AmazonSSM ManagedInstanceCore e AmazonInspector2 a uma função do IAM e anexe essa função à sua instância como um perfil de instância. Para obter instruções sobre como criar e anexar um perfil de instância, consulte Trabalhar com funções do IAM no Guia do usuário do Amazon EC2.

> **Note**
>
> Habilitar a inspeção profunda do Amazon Inspector não é mais um requisito ao executar uma verificação CIS em uma instância. Se você desativar a inspeção profunda, o Amazon Inspector continuará instalando o Agente SSM, mas o plug-in não será mais chamado para executar a inspeção profunda. Isso significa que a seguinte associação estará presente em sua conta:`InspectorLinuxDistributor-do-not-delete`.

## Executando escaneamentos CIS

Você pode executar um escaneamento CIS uma vez sob demanda ou como um escaneamento recorrente agendado. Para executar um escaneamento, primeiro você cria uma configuração de escaneamento.

Ao criar uma configuração de escaneamento, você especifica pares de chave-valor de tag a serem usados nas instâncias de destino. Se você for o administrador delegado do Amazon Inspector para uma organização, você pode especificar várias contas na configuração de escaneamento, e o Amazon Inspector procurará instâncias com as tags especificadas em cada uma dessas contas. Você escolhe o nível de referência do CIS para a verificação. Para cada benchmark, o CIS oferece suporte a perfis de nível 1 e 2 projetados para fornecer linhas de base para diferentes níveis de segurança que diferentes ambientes podem exigir.

- Nível 1 — recomenda configurações básicas essenciais de segurança que podem ser configuradas em qualquer sistema. A implementação dessas configurações deve causar pouca ou nenhuma interrupção do serviço. O objetivo dessas recomendações é reduzir o número de pontos de entrada em seus sistemas, reduzindo os riscos gerais de segurança cibernética.
- Nível 2 — recomenda configurações de segurança mais avançadas para ambientes de alta segurança. A implementação dessas configurações requer planejamento e coordenação para minimizar o risco de impacto nos negócios. O objetivo dessas recomendações é ajudar você a alcançar a conformidade regulatória.

O nível 2 estende o nível 1. Quando você escolhe o Nível 2, o Amazon Inspector verifica todas as configurações recomendadas para os níveis 1 e 2.

Depois de definir os parâmetros do escaneamento, você pode escolher se deseja executá-lo como um escaneamento único, que é executado após a conclusão da configuração, ou como um escaneamento recorrente. As varreduras recorrentes podem ser executadas diariamente, semanalmente ou mensalmente, no horário de sua escolha.

> **Tip**
>
> Recomendamos escolher um dia e hora com menor probabilidade de afetar seu sistema durante a execução da verificação.

Para criar uma configuração de escaneamento CIS

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione Região da AWS onde você deseja executar um escaneamento CIS.
3. No painel de navegação, em Escaneamentos sob demanda, selecione Escaneamentos CIS.
4. Escolha Criar novo escaneamento.
    a. Insira um nome de configuração de digitalização.
    b. Em Target resource, insira a chave e o valor correspondente de uma tag nas instâncias que você deseja verificar. Você pode especificar um total de 25 tags para incluir na digitalização e, para cada chave, você pode especificar até cinco valores diferentes.
    c. Escolha um nível de referência do CIS. Você pode selecionar o Nível 1 para configurações básicas de segurança ou o Nível 2 para configurações avançadas de segurança.
5. Para contas do Target, especifique quais contas incluir na verificação. Uma conta independente ou membro de uma organização pode selecionar Self para criar uma configuração de escaneamento para sua conta. Um administrador delegado do Amazon Inspector pode selecionar Todas as contas para atingir todas as contas dentro da organização ou selecionar Especificar contas e especificar um subconjunto de contas membros a serem segmentadas. O administrador delegado pode inserir, `SELF` em vez de uma ID de conta, para criar uma configuração de escaneamento para sua própria conta. Para obter mais informações, consulte Considerações para gerenciar escaneamentos do Amazon Inspector CIS em uma organização AWS.

6. Escolha um cronograma para os escaneamentos. Escolha entre Escaneamento único, que será executado assim que você terminar de criar a configuração de escaneamento, ou Escaneamentos recorrentes, que serão executados no horário agendado que você escolher até que seja excluído.
7. Escolha Criar para concluir a criação da configuração de escaneamento.

## Visualizando e editando configurações de escaneamento CIS

Você pode visualizar ou editar seus escaneamentos previamente agendados a qualquer momento.

Para visualizar ou editar uma configuração de escaneamento do CIS

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione Região da AWS onde você criou sua configuração de escaneamento do CIS.
3. No painel de navegação, em Escaneamentos sob demanda, selecione Escaneamentos CIS.
4. Escolha Agendado para ver as configurações de escaneamento agendado.
5. Selecione um item na coluna Nome da configuração de escaneamento para abrir os detalhes dessa configuração de escaneamento.
6. (Opcional) Escolha Editar para alterar os parâmetros desse escaneamento.

## Visualizando os resultados de seus escaneamentos do CIS

O Amazon Inspector cria um trabalho de escaneamento toda vez que uma configuração de escaneamento é executada e coleta os resultados do escaneamento sob um ID de escaneamento exclusivo.

Os resultados da verificação ficam disponíveis por 90 dias após a conclusão da verificação. Você pode ver os resultados do escaneamento agregados por cheque ou por recurso de destino.

Resultados do escaneamento agregados por cheques

Os resultados do escaneamento são agrupados por cada verificação individual realizada durante o escaneamento. Para cada verificação, você recebe um relatório de quantos recursos foram aprovados, falharam ou foram ignorados.

Resultados da verificação agregados por recurso

Os resultados do escaneamento são agrupados por cada recurso direcionado pela configuração do escaneamento. Para cada recurso, você recebe um relatório de quais verificações um recurso foi aprovado, falhou ou foi ignorado para esse recurso.

Para ver os resultados do escaneamento

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione Região da AWS onde você deseja visualizar os resultados da digitalização.
3. No painel de navegação, em Escaneamentos sob demanda, selecione Escaneamentos CIS.
4. Selecione o ID do escaneamento do qual você deseja ver os resultados na coluna ID do escaneamento.
5. Escolha como visualizar os resultados do escaneamento:
    - Selecione a guia Verificações para ver os resultados da verificação agregados por verificações.
        - Para uma verificação listada, selecione um número entre aprovado, ignorado ou reprovado na coluna Status do recurso para abrir uma exibição dos recursos filtrados por esse status e por essa verificação.
    - Selecione a guia Recursos escaneados para ver os resultados da verificação agregados por recurso.
        - Selecione um recurso para abrir um painel de detalhes listando as verificações aprovadas, reprovadas ou ignoradas pelo recurso.
6. (Opcional) Use a barra de filtro em qualquer exibição para refinar seus resultados.

Você pode baixar os resultados de uma verificação do CIS usando o console ou a API.

Para baixar os resultados do escaneamento

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione Região da AWS onde você deseja visualizar os resultados da digitalização.
3. No painel de navegação, em Escaneamentos sob demanda, selecione Escaneamentos CIS.
4. Selecione o ID do escaneamento do qual você deseja ver os resultados na coluna ID do escaneamento.

5. Escolha Baixar. Se você for o administrador delegado, poderá optar por baixar os resultados para contas de membros específicas.

# Considerações para gerenciar escaneamentos do Amazon Inspector CIS em uma organização AWS

Ao executar escaneamentos do CIS dentro de uma organização, as contas dos membros e os administradores delegados do Amazon Inspector interagem com as configurações e os resultados do escaneamento do CIS de maneiras diferentes.

Quando um administrador delegado cria uma configuração de verificação do CIS para todas as contas ou uma lista de IDs de contas de membros, a organização é proprietária dessa configuração de verificação. Qualquer que seja a conta do administrador delegado atual, pode gerenciar as configurações de escaneamento de propriedade da organização, mesmo que uma conta diferente as tenha criado. As configurações de escaneamento CIS de propriedade da organização terão um ARN que lista o ID da organização como proprietário, seguindo o padrão:. `arn:aws:inspector2:`*`Region`*`:`*`111122223333`*`:owner/`*`OrganizationId`*`/cis-configuration/`*`scanId`* O ID da conta será o ID da conta de gerenciamento da Organizations.

> **Important**
>
> Você não pode adicionar tags às configurações de escaneamento do CIS de propriedade da organização.

Quando um administrador delegado cria uma configuração de escaneamento e especifica `SELF` como a conta de destino, sua conta possui essa configuração de escaneamento. Mesmo que deixem a organização, ainda poderão gerenciar essa configuração de escaneamento.

> **Note**
>
> Um administrador delegado não pode alterar os alvos de uma configuração de escaneamento que tenha como alvo`SELF`.

As configurações de escaneamento criadas por contas de membros, contas autônomas ou administradores delegados que `SELF` tenham como alvo pertencem à conta que as criou. Essas

configurações de escaneamento CIS têm um ARN que lista essa conta como proprietária seguindo o padrão:. `arn:aws:inspector2:Region:111122223333:owner/111122223333/cis-configuration/scanId` O ID da conta será a conta que criou o escaneamento.

Uma conta de membro em uma organização pode criar configurações de escaneamento para sua própria conta. O administrador delegado pode visualizar as configurações de escaneamento criadas pelos membros, mas não pode editá-las nem excluí-las. Se uma conta membro sair da organização, o administrador delegado não poderá mais ver as configurações de escaneamento criadas por essa conta.

O administrador delegado pode visualizar os resultados da verificação de qualquer conta na organização, incluindo aquelas agendadas pelos membros. Uma conta de membro pode visualizar os resultados de qualquer verificação do CIS em busca de recursos em sua conta, incluindo aquelas agendadas pelo administrador delegado.

## Buckets Amazon S3 de propriedade do Amazon Inspector usados para escaneamentos do Amazon Inspector CIS

O Amazon Inspector atualiza os arquivos de definição da Open Vulnerability and Assessment Language (OVAL) necessários para escaneamentos do CIS. A tabela a seguir lista todos os buckets Amazon S3 de propriedade do Amazon Inspector com definições OVAL que o CIS scan usa de acordo com o suporte. Região da AWS Os buckets devem estar na lista de permissões nas VPCs, se necessário.

> **Note**
>
> Os detalhes de cada um dos seguintes buckets Amazon S3 de propriedade do Amazon Inspector não estão sujeitos a alterações. No entanto, a lista pode ser atualizada para refletir os novos suportes Regiões da AWS. Você não pode usar esses buckets para outras operações do Amazon S3 ou em seus próprios buckets do Amazon S3.

| balde CIS | Região da AWS |
| --- | --- |
| `cis-datasets-prod-arn-5908f6f` | Europe (Stockholm) |
| `cis-datasets-prod-bah-8f88801` | Oriente Médio (Barém) |

| balde CIS | Região da AWS |
| --- | --- |
| cis-datasets-prod-bjs-0f40506 | China (Pequim) |
| cis-datasets-prod-bom-435a167 | Ásia-Pacífico (Mumbai) |
| cis-datasets-prod-cdg-f3a9c58 | Europa (Paris) |
| cis-datasets-prod-cgk-09eb12f | Ásia-Pacífico (Jacarta) |
| cis-datasets-prod-cmh-63030b9 | Leste dos EUA (Ohio) |
| cis-datasets-prod-cpt-02c5c6f | África (Cidade do Cabo) |
| cis-datasets-prod-dub-984936f | Europa (Irlanda) |
| cis-datasets-prod-fra-6eb96eb | Europa (Frankfurt) |
| cis-datasets-prod-gru-de69f99 | América do Sul (São Paulo) |
| cis-datasets-prod-hkg-8e30800 | Ásia-Pacífico (Hong Kong) |
| cis-datasets-prod-iad-8438411 | Leste dos EUA (Norte da Virgínia) |
| cis-datasets-prod-icn-f4eff1c | Ásia-Pacífico (Seul) |
| cis-datasets-prod-kix-5743b21 | Asia Pacific (Osaka) |
| cis-datasets-prod-lhr-8b1fbd0 | Europa (Londres) |
| cis-datasets-prod-mxp-7b1bbce | Europa (Milão) |
| cis-datasets-prod-nrt-464f684 | Ásia-Pacífico (Tóquio) |
| cis-datasets-prod-osu-5bead6f | AWS GovCloud (Leste dos EUA) |
| cis-datasets-prod-pdt-adadf9c | AWS GovCloud (Oeste dos EUA) |
| cis-datasets-prod-pdx-acfb052 | Oeste dos EUA (Oregon) |
| cis-datasets-prod-sfo-1515ba8 | Oeste dos EUA (N. da Califórnia) |

| balde CIS | Região da AWS |
| --- | --- |
| `cis-datasets-prod-sin-309725b` | Ásia-Pacífico (Singapura) |
| `cis-datasets-prod-syd-f349107` | Ásia-Pacífico (Sydney) |
| `cis-datasets-prod-yul-5e0c95e` | Canadá (Central) |
| `cis-datasets-prod-zhy-5a8eacb` | China (Ningxia) |
| `cis-datasets-prod-zrh-67e0e3d` | Europa (Zurique) |

# Avaliar a cobertura do Amazon Inspector sobre seu ambiente da AWS

Para ajudá-lo a avaliar e interpretar a cobertura do seu AWS ambiente pelo Amazon Inspector, a página de gerenciamento de contas no console do Amazon Inspector fornece estatísticas e detalhes sobre o status da verificação do Amazon Inspector em suas contas e recursos. Com essa página, você poderá revisar estatísticas agregadas e outros dados de seus recursos. Você também poderá realizar uma análise aprofundada da cobertura do Amazon Inspector para recursos individuais e detalhar para analisar as descobertas de recursos específicos. Se você for o administrador delegado do Amazon Inspector para uma organização, os dados incluem estatísticas e detalhes de todas as contas em sua organização.

Para avaliar a cobertura do Amazon Inspector sobre seu ambiente AWS

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. No painel de navegação, selecione Gerenciamento de contas.
3. Na página Gerenciamento de contas, escolha a guia para uma das cinco visualizações de cobertura diferentes:

    - Contas, para cobertura em nível de conta.
    - Instâncias, para cobertura de instâncias do Amazon Elastic Compute Cloud (Amazon EC2).
    - Repositórios, para cobertura de repositórios do Amazon Elastic Container Registry (Amazon ECR).
    - Imagens, para cobertura de imagens de contêineres do Amazon ECR.
    - Lambda, para cobertura das funções do Lambda.

Os tópicos desta seção descrevem as informações que cada guia fornece, incluindo o status de verificação que um recurso individual pode ter.

Tópicos

- Avaliação da cobertura das funções AWS Lambda

# Avaliar a cobertura em nível de conta

Se sua conta não faz parte de uma organização ou não é a conta delegada de administrador do Amazon Inspector para uma organização, o guia Contas fornece informações sobre sua conta e o status da verificação de recursos para sua conta. Nesse guia, você poderá ativar ou desativar a verificação de todos ou somente tipos específicos de recursos da sua conta. Para ter mais informações, consulte Verificação automatizada de recursos do Amazon Inspector.

Se sua conta for a conta delegada de administrador do Amazon Inspector para uma organização, o guia Contas fornece configurações de ativação automática para contas em sua organização e lista todas as contas em sua organização. Para cada conta, a lista indica se o Amazon Inspector está ativado para a conta e, em caso afirmativo, os tipos de verificação de recursos que estão ativados para a conta. Como administrador delegado, use essa guia para alterar as configurações de ativação automática da sua organização. Você também poderá ativar ou desativar tipos específicos de verificação de recursos para contas de membros individuais. Para ter mais informações, consulte Habilitar verificações de contas-membro do Amazon Inspector.

# Avaliar a cobertura das instâncias do Amazon EC2

O guia Instâncias mostra instâncias do Amazon EC2 em seu ambiente AWS . As listas são organizadas em grupos nos seguintes guias:

- Tudo: mostra todas as instâncias em seu ambiente. A coluna Status indica o status atual da verificação de uma instância.
- Verificação: mostra todas as instâncias que o Amazon Inspector está monitorando e verificando ativamente em seu ambiente.
- Sem verificação: mostra todas as instâncias que o Amazon Inspector não está monitorando e verificando em seu ambiente. A coluna Motivo indica por que o Amazon Inspector não está monitorando e verificando uma instância.

  Uma instância do EC2 pode aparecer no guia Não verificar por vários motivos. O Amazon Inspector usa AWS Systems Manager (SSM) e o agente SSM para monitorar e verificar automaticamente suas instâncias do EC2 em busca de vulnerabilidades. Se uma instância não tiver o Agente SSM em execução, não tiver uma função AWS Identity and Access Management (IAM) compatível com o Systems Manager ou não estiver executando um sistema operacional ou

uma arquitetura compatível, o Amazon Inspector não poderá monitorar e escanear a instância. Para ter mais informações, consulte Verificar as instâncias do Amazon EC2.

Em cada guia, a coluna Conta especifica quem é dono Conta da AWS de uma instância.

Tags de instância do EC2 — Esta coluna mostra as tags associadas à instância e pode ser usada para determinar se a instância foi excluída das verificações por tags.

Sistema operacional — Esta coluna mostra o tipo de sistema operacional, que pode ser `WINDOWS`, `MAC`, `LINUX` ou `UNKNOWN`.

Uso monitorado — Esta coluna mostra se o Amazon Inspector está usando o método de verificação baseado em agente ou sem agente na instância.

Última verificação — Esta coluna mostra quando o Amazon Inspector verificou pela última vez vulnerabilidades nesse recurso. A frequência com que o Amazon Inspector executa verificações depende do método de verificação usado para verificar a instância.

Para analisar detalhes adicionais sobre uma instância do EC2, escolha o link na coluna da instância do EC2. Em seguida, o Amazon Inspector exibe detalhes sobre a instância e as descobertas atuais da instância. Para revisar os detalhes de uma descoberta, escolha o link na coluna Título. Para obter informações detalhadas, consulte o Detalhes da descoberta do Amazon Inspector.

## Escaneamento de valores de status para instâncias do Amazon EC2

Para uma instância do Amazon Elastic Compute Cloud (Amazon EC2), os possíveis valores de Status são:

- Monitoramento ativo: o Amazon Inspector monitora e verifica continuamente a instância.
- Instância do EC2 interrompida: o Amazon Inspector pausou a verificação da instância porque ela está em um estado interrompido. Todas as descobertas existentes persistirão até que a instância seja encerrada. Se a instância for reiniciada, o Amazon Inspector retomará automaticamente a verificação da instância.
- Erro interno: ocorreu um erro interno quando o Amazon Inspector tentou verificar a instância. O Amazon Inspector resolverá automaticamente o erro e retomará a verificação assim que possível.
- Sem inventário: o Amazon Inspector não conseguiu encontrar o inventário do aplicativo de software para verificar a instância. As associações do Amazon Inspector para a instância podem ter sido excluídas ou podem ter falhado na execução.

Para corrigir esse problema, use AWS Systems Manager para garantir que a `InspectorInventoryCollection-do-not-delete` associação exista e que seu status de associação seja bem-sucedido. Além disso, use o AWS Systems Manager do Gerenciador de Frotas para verificar o inventário de aplicativos de software da instância.

- Desativação pendente: o Amazon Inspector parou de verificar a instância. A instância está sendo desativada, aguardando a conclusão das tarefas de limpeza.
- Verificação inicial pendente: o Amazon Inspector colocou a instância em fila para uma verificação inicial.
- Recurso encerrado: a instância foi encerrada. No momento, o Amazon Inspector está limpando as descobertas existentes e os dados de cobertura da instância.
- Inventário obsoleto: o Amazon Inspector não conseguiu coletar um inventário atualizado de aplicativos de software que foi capturado nos últimos 7 dias para a instância.

  Para remediar esse problema, use AWS Systems Manager para garantir que as associações necessárias do Amazon Inspector existam e estejam em execução para a instância. Além disso, use o AWS Systems Manager do Gerenciador de Frotas para verificar o inventário de aplicativos de software da instância.
- Instância EC2 não gerenciada: o Amazon Inspector não está monitorando ou verificando a instância. A instância não é gerenciada pelo AWS Systems Manager.

  Para corrigir esse problema, você pode usar o AWSSupport-TroubleshootManagedInstance runbookfornecido pela AWS Systems Manager Automation. Depois de configurar AWS Systems Manager para gerenciar a instância, o Amazon Inspector começará automaticamente a monitorar e escanear continuamente a instância.
- Sistema operacional não compatível: o Amazon Inspector não está monitorando nem verificando a instância. A instância usa um sistema operacional ou arquitetura que o Amazon Inspector não dá suporte. Para obter uma lista dos sistemas operacionais que o Amazon Inspector com suporte, consulte Sistemas operacionais com suporte ao escaneamento do Amazon EC2.
- Monitoramento ativo com erros parciais: esse status significa que a verificação do EC2 está ativa, mas há erros associados com Inspeção detalhada do Amazon Inspector para instâncias do Amazon EC2 Linux. Os possíveis erros de inspeção profunda são:
  - Limite de coleta de pacotes de inspeção profunda excedido — A instância excedeu o limite de 5000 pacotes para a inspeção profunda do Amazon Inspector. Para retomar a inspeção profunda dessa instância, você pode tentar ajustar os caminhos personalizados associados à conta.

- Inspeção profunda: limite diário de inventário SSM excedido — O agente SSM não conseguiu enviar inventário para o Amazon Inspector porque a cota de SSM para dados de inventário coletados por instância por dia já foi atingida para essa instância. Para obter mais informações, consulte os Endpoints e cotas do Gerenciador de Sistemas do Amazon EC2.
- Limite de tempo de coleta de inspeção profunda excedido — O Amazon Inspector não conseguiu extrair o inventário do pacote porque o tempo de coleta do pacote excedeu o limite máximo de 15 minutos.
- A inspeção detalhada não tem inventário — O plug-in Amazon Inspector SSM ainda não conseguiu coletar um inventário de pacotes para esta instância. Isso geralmente é o resultado de uma verificação pendente, no entanto, se esse status persistir após 6 horas, use o Gerenciador de sistemas do Amazon EC2 para garantir que as associações necessárias do Amazon Inspector existam e estejam em execução para a instância.

Para obter detalhes sobre como definir as configurações de verificação para uma instância do EC2, consulte Verificar as instâncias do Amazon EC2.

## Avaliar a cobertura dos repositórios do Amazon ECR

O guia Repositórios mostra os repositórios do Amazon ECR em seu ambiente da AWS . As listas são organizadas em grupos nos guias a seguir:

- Tudo: mostra todos os repositórios em seu ambiente. A coluna Status indica o status atual da verificação de um repositório.
- Ativado: mostra todos os repositórios que o Amazon Inspector está configurado para monitorar e verificar em seu ambiente. A coluna Status indica o status atual da verificação de um repositório.
- Não ativado: mostra todos os repositórios que o Amazon Inspector não está monitorando e verificando em seu ambiente. A coluna Motivo indica por que o Amazon Inspector não está monitorando e verificando um repositório.

Em cada guia, a coluna Conta especifica quem possui um repositório. Conta da AWS

Para revisar detalhes adicionais sobre um repositório, escolha o nome do repositório. Em seguida, o Amazon Inspector exibe uma lista de imagens de contêineres no repositório e detalhes de cada imagem. Os detalhes incluem a etiqueta da imagem, o resumo da imagem e o status da verificação. Eles também incluem estatísticas de descobertas importantes, como o número de descobertas

críticas da imagem. Para detalhar e revisar os dados de suporte de estatísticas de descobertas, escolha a tag de imagem para a imagem.

## Valores de status de digitalização para repositórios do Amazon ECR

Para um repositório do Amazon Elastic Container Registry (Amazon ECR), os valores de status possíveis são:

- Ativado (contínuo) — Para um repositório, o Amazon Inspector monitora continuamente as imagens nesse repositório. A configuração de escaneamento avançado para o repositório está definida como verificação contínua. O Amazon Inspector digitaliza inicialmente novas imagens quando elas são enviadas e digitaliza novamente as imagens se um novo CVE relevante para essa imagem for publicado. O Amazon Inspector continuará monitorando imagens neste repositório durante a duração do escaneamento ECR que você configurar.
- Ativado (por envio) — O Amazon Inspector digitaliza automaticamente imagens de contêineres individuais no repositório quando uma nova imagem é enviada. O escaneamento aprimorado é ativado para o repositório e configurado para escanear por push.
- Acesso negado: o Amazon Inspector não tem permissão para acessar o repositório ou qualquer imagem de contêiner no repositório.

  Para remediar esse problema, certifique-se de que as políticas AWS Identity and Access Management (IAM) para o repositório permitam que o Amazon Inspector acesse o repositório.
- Desativado (Manual): o Amazon Inspector não está monitorando nem verificando nenhuma imagem de contêiner no repositório. A configuração de escaneamento do Amazon ECR para o repositório está definida como verificação manual básica.

  Para começar a verificar imagens no repositório com o Amazon Inspector, altere a configuração de verificação do repositório para escaneamento avançado e, em seguida, escolha se deseja verificar imagens continuamente ou somente quando uma nova imagem for enviada.
- Ativado (por envio) — O Amazon Inspector digitaliza automaticamente imagens de contêineres individuais no repositório quando uma nova imagem é enviada. A configuração de escaneamento avançado do repositório está definida para verifcar por push.
- Erro interno — Ocorreu um erro interno quando o Amazon Inspector tentou escanear o repositório. O Amazon Inspector resolverá automaticamente o erro e retomará a verificação assim que possível.

Para obter detalhes sobre como definir as configurações de escaneamento para repositóriosVerificar imagens de contêiner do Amazon ECR.

# Avaliar a cobertura de imagens de contêiner do Amazon ECR

O guia Imagens mostra imagens de contêineres do Amazon ECR em seu ambiente da AWS . As listas são organizadas em grupos nos guias a seguir:

- Tudo: mostra todas as imagens de contêineres em seu ambiente. A coluna Status indica o status atual da verificação de uma imagem.
- Verificação: mostra todas as imagens de contêineres que o Amazon Inspector está configurado para monitorar e verificar em seu ambiente. A coluna Status indica o status atual da verificação de uma imagem.
- Sem verificação: mostra todas as imagens de contêineres que o Amazon Inspector não está monitorando e verificando em seu ambiente. A coluna Motivo indica por que o Amazon Inspector não está monitorando e verificando uma imagem.

  Uma imagem de contêiner pode aparecer no guia Não ativada por vários motivos. A imagem pode ser armazenada em um repositório para o qual as verificações do Amazon Inspector não estão ativadas, ou as regras de filtragem do Amazon ECR impedem que esse repositório seja verificado. Ou a imagem não foi enviada ou retirada dentro do número de dias que você configurou para a duração da nova digitalização do ECR. Para ter mais informações, consulte Configurando a duração da nova digitalização do ECR.

Em cada guia, a coluna Nome do repositório especifica o nome do repositório que armazena uma imagem de contêiner. A coluna Conta especifica quem é Conta da AWS o proprietário do repositório. A coluna Última verificação mostra quando o Amazon Inspector verificou pela última vez esse recurso em busca de vulnerabilidades. Isso pode incluir verificações quando há uma atualização na descoberta de metadados, quando há uma atualização no inventário de aplicativos do recurso ou quando uma nova verificação é feita em resposta a uma nova CVE. Para ter mais informações, consulte Comportamentos de verificação para o escaneamento do Amazon ECR.

Para revisar detalhes adicionais sobre uma imagem de contêiner, escolha o link na coluna de Imagem de contêiner do ECR. Em seguida, o Amazon Inspector exibe detalhes sobre a imagem e as descobertas atuais da imagem. Para revisar os detalhes de uma descoberta, escolha o link na coluna Título. Para obter informações detalhadas, consulte o Detalhes da descoberta do Amazon Inspector.

# Valores de status de digitalização para imagens de contêineres do Amazon ECR

Para uma imagem de contêiner do Amazon Elastic Container Registry, os valores de status possíveis são:

- Monitoramento ativo (contínuo) — O Amazon Inspector monitora continuamente e a imagem e novas digitalizações são realizadas nela sempre que um novo CVE relevante é publicado. A duração da redigitalização do Amazon ECR para a imagem é atualizada sempre que a imagem é empurrada ou puxada. O escaneamento avançado é ativado para o repositório que armazena a imagem, e a configuração de verificação avançada para o repositório está definida como verificação contínua.
- Ativado (ao enviar) — O Amazon Inspector digitaliza automaticamente a imagem sempre que uma nova imagem é enviada. O escaneamento avançado é ativado para o repositório que armazena a imagem, e a configuração de escaneamento avançado do repositório está definida para verificar por push.
- Erro interno — Ocorreu um erro interno quando o Amazon Inspector tentou escanear a imagem do contêiner. O Amazon Inspector resolverá automaticamente o erro e retomará a verificação assim que possível.
- Escaneamento inicial pendente — O Amazon Inspector colocou a imagem em fila para um escaneamento inicial.
- A elegibilidade da digitalização expirou (contínua) — O Amazon Inspector suspendeu a digitalização da imagem. A imagem não foi atualizada dentro do período que você especificou para novas verificações automáticas de imagens no repositório. Você pode empurrar ou puxar a imagem para continuar a digitalização.
- A elegibilidade do escaneamento expirou (On push) — O Amazon Inspector suspendeu a digitalização da imagem. A imagem não foi atualizada dentro do período que você especificou para novas verificações automáticas de imagens no repositório. Você pode pressionar a imagem para continuar a digitalização.
- Manual de frequência de verificação (Manual): o Amazon Inspector não verifica a imagem do contêiner Amazon ECR. A configuração de escaneamento do Amazon ECR para o repositório que armazena a imagem está definida como verificação manual básica. Para começar a verificar a imagem automaticamente com o Amazon Inspector, altere a configuração do repositório para o escaneamento avançado e, em seguida, escolha se deseja verificar imagens de maneira contínua ou somente quando uma nova imagem for enviada.

- Sistema operacional não suportado — O Amazon Inspector não está monitorando ou digitalizando a imagem. A imagem é baseada em um sistema operacional não compatível com o Amazon Inspector ou contém um tipo de mídia não compatível com o Amazon Inspector.

  Para ver uma lista de sistemas operacionais compatíveis com o Amazon Inspector, consulte Sistemas operacionais com suporte ao escaneamento do Amazon ECR. Para ver uma lista dos tipos de mídia compatíveis com o Amazon Inspector, consulte Tipos de mídia compatíveis.

Para obter detalhes sobre como definir as configurações de verificação para repositórios e imagens, consulte Verificar imagens de contêiner do Amazon ECR.

## Avaliação da cobertura das funções AWS Lambda

A guia Lambda mostra as funções do Lambda em seu ambiente. AWS Nesta página, duas tabelas, uma que mostra detalhes da cobertura da função para o escaneamento padrão do Lambda e outra para o escaneamento de código do Lambda. Agrupe funções com base nos seguintes guias:

- Tudo: mostra todas as funções do Lambda em seu ambiente. A coluna Status indica o status atual da verificação de uma função do Lambda.
- Verificação: mostra as funções do Lambda que o Amazon Inspector está configurado para verificar. A coluna Status indica o status atual da verificação de cada função do Lambda.
- Sem verificação: mostra as funções do Lambda que o Amazon Inspector não está configurado para verificar. A coluna Motivo indica por que o Amazon Inspector não está monitorando e verificando uma função.

  Uma função do Lambda pode aparecer no guia Sem verificação por vários motivos. A função do Lambda pode pertencer a uma conta que não foi adicionada ao Amazon Inspector ou as regras de filtragem impedem que essa função seja verificada. Para ter mais informações, consulte AWS Lambda Funções de digitalização.

Em cada guia, a coluna Nome da função especifica o nome da função do Lambda. A coluna Conta especifica Conta da AWS o proprietário da função. O identificador do runtime da função. A coluna Status indica o status atual da verificação de cada função do Lambda. Tags de recursos mostram as tags que foram aplicadas à função. A coluna Última verificação mostra quando o Amazon Inspector verificou pela última vez esse recurso em busca de vulnerabilidades. Isso pode incluir verificações quando há uma atualização na descoberta de metadados, quando há uma atualização no inventário de aplicativos do recurso ou quando uma nova verificação é feita em resposta a uma nova CVE.

Para ter mais informações, consulte Comportamentos de verificação para escaneamento de funções do Lambda.

## Valores de status de digitalização para AWS Lambda funções

Para uma função do Lambda, os valores de Status possíveis são:

- Monitoramento ativo: o Amazon Inspector monitora e verifica continuamente as funções do Lambda. A verificação contínua inclui uma verificação inicial de novas funções quando são enviadas para o repositório e novas verificações automatizadas de funções quando atualizadas ou quando novas CVEs (vulnerabilidades e exposições comuns) são lançadas.
- Excluído por tag: o Amazon Inspector não está verificando essa função porque ela foi excluída dos verificações por tags.
- A elegibilidade da verificação expirou: o Amazon Inspector não está monitorando essa função porque já passaram 90 dias ou mais desde a última vez que ela foi invocada ou atualizada.
- Erro interno: ocorreu um erro interno quando o Amazon Inspector tentou verificar a função. O Amazon Inspector resolverá automaticamente o erro e retomará a verificação assim que possível.
- Verificação inicial pendente: o Amazon Inspector colocou a função em fila para um verificação inicial.
- Sem suporte: a função do Lambda tem um runtime incompatível.

# Gerenciando várias contas no Amazon Inspector com Organizations

Você pode usar o Amazon Inspector para gerenciar várias contas associadas por meio de Organizations AWS . Para gerenciar várias contas do Amazon Inspector, a conta de gerenciamento do Organizations designa uma conta dentro da organização como a conta de administrador delegado do Amazon Inspector. O administrador delegado gerencia o Amazon Inspector para a organização e recebe permissões especiais para executar tarefas em nome de sua organização. Essas tarefas incluem ativar ou desativar escaneamentos de contas de membros, visualizar dados agregados de localização de toda a organização e criar e gerenciar regras de supressão.

> **Note**
>
> Para habilitar programaticamente o Amazon Inspector para várias contas em Regiões da AWS várias, você pode usar um script de shell desenvolvido pelo Amazon Inspector. Para obter mais informações sobre como usar esse script, consulte inspector2- enablement-with-cli no GitHub site.

Tópicos



## Noções básicas sobre o relacionamento entre as contas de administrador e de membro do Amazon Inspector

Quando você usa o Amazon Inspector em um ambiente de várias contas, a conta de administrador delegado do Amazon Inspector tem acesso a determinados metadados. Esses metadados incluem dados de configuração do Amazon EC2 e do Amazon ECR e resultados de descobertas de segurança para contas de membros. A conta do administrador também pode criar regras de supressão de descoberta que são aplicadas às contas dos membros. Para ter mais informações, consulte Suprimir descobertas do Amazon Inspector com regras de supressão.

# Ações de administrador delegado

Geralmente, quando o administrador delegado aplica configurações à sua conta, essas configurações são aplicadas a todas as outras contas na organização. O administrador delegado também pode visualizar e recuperar informações da própria conta e de qualquer membro associado. Uma conta de administrador delegado do Amazon Inspector pode executar as seguintes ações:

- Visualize e gerencie o status do Amazon Inspector para contas associadas, incluindo a ativação e a desativação do Amazon Inspector.
- Habilitar ou desabilitar tipos de verificação para todas as contas-membro da organização.
- Visualize dados agregados de descoberta em toda a organização e detalhes de localização de todas as contas de membros da organização.
- Crie e gerencie regras de supressão que sejam aplicáveis às descobertas de todas as contas na organização.
- Ative o escaneamento aprimorado do Amazon ECR para todos os membros da organização.
- Veja a cobertura de recursos para toda a organização.
- Defina a duração para verificações automáticas de imagens de contêiner do ECR para todas as contas-membro da organização. A configuração de duração do escaneamento do administrador delegado substitui qualquer configuração definida anteriormente pela conta do membro. Todas as contas da organização compartilham a duração de nova verificação automática do Amazon ECR dos administradores delegados. Você não pode definir durações de nova verificação diferentes para contas individuais.
- Especifique cinco caminhos personalizados para a inspeção profunda do Amazon Inspector para o Amazon EC2, que serão usados em todas as contas da organização. Eles são um acréscimo aos cinco caminhos personalizados que um administrador delegado pode definir para sua conta individual. Para obter mais informações sobre como configurar caminhos personalizados de inspeção profunda, consulteCaminhos personalizados para a inspeção profunda do Amazon Inspector.
- Ative e desative a inspeção profunda do Amazon Inspector para contas de membros.
- Exporte SBOMs para qualquer conta de membro da organização.
- Defina o modo de verificação do Amazon EC2 para todas as contas de membro da organização. Para ter mais informações, consulte Gerenciar o modo de digitalização.
- Crie e gerencie configurações de escaneamento CIS para todas as contas na organização, exceto para quaisquer configurações de escaneamento criadas por contas de membros.

> **Note**
>
> Se uma conta membro sair da organização, o administrador delegado não poderá mais ver as configurações de escaneamento agendadas por essa conta.

- Veja os resultados da verificação do CIS para todas as contas na organização.

## Ações da conta de membro

Uma conta de membro pode visualizar e recuperar informações sobre sua conta no Amazon Inspector, enquanto as configurações de sua conta são gerenciadas pelo administrador delegado. As contas de membro de uma empresa podem executar as seguintes ações no Amazon Inspector:

- Ativar os escaneamentos do Amazon Inspector para sua conta.
- Visualizar a cobertura de recursos para sua própria conta.
- Visualizar os detalhes das descobertas para sua conta.
- Visualizar a configuração de duração da nova digitalização automática da imagem do contêiner ECR para sua conta.
- Especifique cinco caminhos personalizados para a inspeção profunda do Amazon Inspector para EC2 que serão usados para sua conta individual. Esses caminhos são escaneados, além de qualquer caminho personalizado que o administrador delegado tenha especificado para a organização. Para obter mais informações sobre como configurar caminhos de inspeção profunda, consulteCaminhos personalizados para a inspeção profunda do Amazon Inspector.
- Veja os caminhos personalizados definidos pelo seu administrador delegado para a inspeção profunda do Amazon Inspector.
- Exporte SBOMs para qualquer recurso associado à conta.
- Visualize o modo de verificação da conta.
- Crie e gerencie as configurações de escaneamento do CIS para sua conta.
- Veja os resultados de qualquer verificação do CIS em busca de recursos em sua conta, incluindo aquelas agendadas pelo administrador delegado.

> **Note**
>
> Após a ativação, o Amazon Inspector pode ser desativado somente por uma conta de administrador delegado.

# Desabilitar um administrador delegado do Amazon Inspector

## Considerações importantes para administradores delegados

Os seguintes fatores que definem como o administrador delegado opera no Amazon Inspector:

Um administrador delegado pode gerenciar no máximo 5 mil membros.

Cada administrador delegado do Amazon Inspector tem uma cota de 5 mil contas de membros. No entanto, pode haver mais de 5 mil contas em sua organização. Se você ultrapassar 5.000 contas de membros, receberá uma notificação por meio do Amazon CloudWatch Personal Health Dashboard e um e-mail para a conta do administrador delegado.

Um administrador delegado é regional.

Ao contrário AWS Organizations, o Amazon Inspector é um serviço regional. Isso significa que você deve designar um administrador delegado, adicionar contas de membros e ativar os tipos de escaneamento em cada um em Região da AWS que você deseja usar o Amazon Inspector.

Uma organização pode ter apenas um administrador delegado.

Você só pode ter um administrador delegado do Amazon Inspector para uma organização. Se você designou uma conta como administrador delegado em uma região, essa conta deve ser seu administrador delegado em todas as outras regiões.

Alterar um administrador delegado não desativa o Amazon Inspector para contas de membros.

Se você remover o administrador delegado, o Amazon Inspector não será desativado nessas contas e as configurações de digitalização não serão afetadas.

Sua AWS organização deve ter todos os recursos ativados.

Essa é a configuração padrão para AWS Organizations. Se não estiver ativado, consulte Ativação de todos os recursos em sua organização.

## Permissões necessárias para designar um administrador delegado

Você deve ter permissão para ativar o Amazon Inspector e designar um administrador delegado do Amazon Inspector.

Adicione a seguinte instrução ao final de uma política do IAM para conceder essas permissões:

```
{
    "Sid": "PermissionsForInspectorAdmin",
    "Effect": "Allow",
    "Action": [
        "inspector2:EnableDelegatedAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
    ],
    "Resource": "*"
}
```

## Designar um administrador delegado para sua organização AWS

O procedimento a seguir mostra como designar um administrador delegado para sua AWS organização. Quando essa designação é concluída, o Amazon Inspector é ativado tanto para a conta de gerenciamento do Organizações quanto para a conta de administrador delegado escolhida.

> **Note**
>
> Somente a conta de gerenciamento do Organizações pode designar um administrador delegado.

Ativar o Amazon Inspector pela primeira vez cria a função vinculada ao serviço (`SLRAWSServiceRoleForAmazonInspector`) para a conta. Para obter mais informações sobre como Amazon Inspector usa as funções vinculadas ao serviço, consulte Uso de funções vinculadas a serviço para o Amazon Inspector. Para obter mais informações sobre funções vinculadas a serviços, consulte Usar funções vinculadas a serviços no Guia do usuário do IAM.

Designar um administrador delegado do Amazon Inspector

Console

Designar um administrador delegado no console

1. Faça login no AWS Management Console usando a conta AWS Organizations de gerenciamento.
2. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home e use o Região da AWS seletor no canto superior direito para especificar a região na qual você deseja designar um administrador.
3. No painel Administrador delegado, insira o ID da conta de doze dígitos do Conta da AWS que você deseja designar como administrador delegado do Amazon Inspector para sua organização. Em seguida, escolha Delegar administração.
4. (Recomendado) Repita as etapas anteriores em cada Região da AWS.

API

Designar um administrador delegado usando a API

- Execute a operação EnableDelegatedAdminAccountda API usando as credenciais da conta Conta da AWS de gerenciamento da Organizations. Você também pode usar o AWS Command Line Interface para fazer isso executando o seguinte comando CLI:. `aws inspector2 enable-delegated-admin-account --delegated-admin-account-id 11111111111`

  > **Note**
  >
  > Certifique-se de especificar o ID da conta que você deseja tornar um administrador delegado do Amazon Inspector.

Depois de especificar o administrador delegado, você deve usar a conta AWS Organizations de gerenciamento somente para alterar ou remover a conta do administrador delegado.

# Habilitar verificações de contas-membro do Amazon Inspector

Como administrador delegado da sua organização, ative o escaneamento do Amazon EC2, o escaneamento do Amazon ECR ou os dois para qualquer membro associado à conta de gerenciamento do AWS Organizations . Ao ativar escaneamentos para uma conta membro, essa conta se torna associada ao administrador delegado, o Amazon Inspector é ativado automaticamente e os escaneamentos do tipo escolhido são iniciados imediatamente. Para obter informações sobre quais recursos podem ser verificados e como configurar escaneamentos, consulte. Verificação automatizada de recursos do Amazon Inspector

O Amazon Inspector fornece várias opções para gerenciar e ativar escaneamentos para contas de membros, incluindo permitir que contas de membros ativem o Amazon Inspector. Utilize uma das seguintes opções para iniciar verificações para contas-membro.

Para ativar automaticamente a verificação de todas as contas de membros

1. Faça login na conta do administrador delegado.
2. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home. Em seguida, use o Região da AWS seletor no canto superior direito para especificar a região na qual você deseja ativar o escaneamento de todas as contas dos membros.
3. No painel de navegação, em Configurações, selecione Gerenciamento de contas. A tabela de contas exibe todas as contas de membros associadas à conta AWS Organizations de gerenciamento.
4. Marque a caixa de seleção na parte superior da tabela para selecionar todas as contas nesta página. Em seguida, escolha Ativar e selecione sua opção de tipo de digitalização preferida no menu.

   > **Note**
   >
   > Somente as contas atualmente visíveis na página são selecionadas. Se você tiver várias páginas de contas, deverá repetir esse processo em cada página. Para alterar o número de contas exibidas na página, selecione o ícone de roda dentada.

5. Ative a configuração Ativar automaticamente o Inspector para novas contas de membros e, em seguida, selecione os tipos de escaneamento para ativar quaisquer novos membros adicionados à sua organização.

6. (Recomendado) Repita essas etapas em cada região em que você deseja verificar as contas dos membros.

A configuração Ativar automaticamente o Inspetor para novas contas de membros ativa o Amazon Inspector para todos os futuros membros da sua organização. Isso permite que o administrador delegado do Amazon Inspector gerencie quaisquer novos membros criados ou adicionados à organização. Quando o número de contas de membros atinge a cota de 5.000, essa configuração é automaticamente desativada. Se uma conta for removida e o número total de membros diminuir para menos de 5 mil, a configuração será reativada automaticamente.

Para ativar seletivamente as contas dos membros

1. Faça login na conta do administrador delegado.
2. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home e, em seguida, use o Região da AWS seletor no canto superior direito para especificar a região na qual você deseja ativar a verificação de determinadas contas membros.
3. No painel de navegação, em Configurações, selecione Gerenciamento de contas. A tabela de contas exibe todas as contas de membros associadas à conta AWS Organizations de gerenciamento.
4. Na página de gerenciamento de conta, marque a caixa de seleção para cada conta membro para a qual deseja ativar a verificação.
5. Selecione Ativar.
6. No menu Ativar, escolha os tipos de escaneamento a serem ativados para as contas selecionadas. Você pode escolher entre as seguintes opções:
   - Todos os escaneamentos — para ativar todos os tipos de escaneamento.
   - Escaneamento EC2 — para ativar escaneamentos de instâncias do Amazon EC2.
   - Digitalização de contêineres ECR — para ativar digitalizações de imagens de contêineres ECR.
   - AWS Lambda digitalização padrão — para ativar escaneamentos de funções Lambda.
7. (Recomendado) Repita essas etapas em cada região em que você deseja ativar escaneamentos para determinados membros.

Se a sua conta AWS Organizations de gerenciamento delegou um administrador para o Amazon Inspector, você pode ativar sua própria conta como membro e ver os detalhes do escaneamento de sua própria conta.

Para ativar o escaneamento como conta de membro

1. Faça login na sua conta.
2. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home e use o Região da AWS seletor no canto superior direito para especificar a região na qual você deseja ativar o escaneamento.
3. No painel de navegação, em Configurações, selecione Gerenciamento de contas.
4. Na página Gerenciamento da conta, marque a caixa de seleção da conta.
5. No menu Ativar, escolha os tipos de escaneamento a serem ativados. Você pode escolher entre as seguintes opções:
   - Todos os escaneamentos — para ativar todos os tipos de escaneamento.
   - Escaneamento EC2 — para ativar escaneamentos de instâncias do Amazon EC2.
   - Digitalização de contêineres ECR — para ativar digitalizações de imagens de contêineres ECR.
   - AWS Lambda digitalização padrão — para ativar escaneamentos de funções Lambda.
6. (Recomendado) Repita essas etapas em cada região em que você deseja ativar os escaneamentos.

## Desassociar contas-membro no Amazon Inspector

O procedimento a seguir mostra como desassociar contas-membro. As contas de membros dissociadas permanecem em sua AWS Organizations organização como contas autônomas do Amazon Inspector. O administrador delegado do Amazon Inspector não tem mais permissão para ativar e gerenciar o Amazon Inspector para essas contas. Você pode adicionar contas desassociadas como membros novamente mais tarde.

> **Note**
>
> Desassociar uma conta não desativa os escaneamentos do Amazon Inspector para essa conta.

Console

Para desassociar contas de membro usando o console

1. Faça login na conta de administrador delegado.
2. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home e use o Região da AWS seletor no canto superior direito para especificar a região na qual você deseja desassociar uma ou mais contas membros.
3. No painel de navegação, em Configurações, selecione Gerenciamento de contas.
4. Na página Gerenciamento de conta, marque a caixa de seleção para cada conta que deseja desassociar.
5. No menu Ações, escolha Desassociar conta.
6. (Recomendado) Repita essas etapas em cada região em que você deseja desassociar contas.

API

Para desassociar contas de membro usando a API

Execute a operação DisassociateMember da API. Na solicitação, forneça os IDs da conta que você está desassociando.

## Removendo um administrador delegado do Amazon Inspector

Se você precisar atribuir um novo administrador delegado do Amazon Inspector, você pode remover um administrador delegado existente como conta de gerenciamento. AWS Organizations

Quando você remove um administrador delegado, ele não desativa o Amazon Inspector nessa conta ou em qualquer conta membro da organização. As contas em sua organização são convertidas em contas autônomas e mantêm as configurações de verificação que tinham antes de serem gerenciadas por um administrador delegado.

Para remover um administrador delegado

1. Faça login no AWS Management Console usando a conta AWS Organizations de gerenciamento.

2. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home e use o Região da AWS seletor no canto superior direito para especificar a região da qual você deseja remover o administrador delegado.
3. No painel de navegação, em Configurações, selecione Gerenciamento de contas.
4. Na seção Administrador delegado, escolha Remover e confirme sua ação.
5. Repita essas etapas em cada região em que você registrou esse administrador delegado.

Ao adicionar um novo administrador delegado do Amazon Inspector, você deve associar manualmente os membros da organização à nova conta de administrador. Use as etapas a seguir para associar membros da organização à nova conta de administrador.

Para associar membros a um novo administrador delegado

1. Faça login no AWS Management Console usando a conta de administrador delegado.
2. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home e use o Região da AWS seletor no canto superior direito para especificar a região na qual você deseja associar membros ao novo administrador delegado.
3. No painel de navegação, em Configurações, selecione Gerenciamento de contas.
4. Selecione todas as contas listadas em sua organização usando a caixa de seleção superior.
5. No menu Ações, escolha Adicionar membros.
6. Repita essas etapas em cada região na qual você deseja associar membros ao novo administrador delegado.

# Monitorar de uso e custo no Amazon Inspector

Use o console do Amazon Inspector e as operações de API para projetar os custos mensais do uso do Amazon Inspector em seu ambiente. Se for o administrador do Amazon Inspector de um ambiente com várias contas, você poderá visualizar o custo total de todo o o ambiente e as métricas de custo de cada uma das contas membros.

## Usar o console de uso

É possível avaliar o uso e o custo projetado do Amazon Inspector a partir do console.

Para acessar as estatísticas de uso

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. Usando o Região da AWS seletor no canto superior direito da página, selecione a região na qual você deseja monitorar os custos.
3. No painel de navegação, selecione Uso.

Na guia Por conta, você verá o custo total projetado com base no período de 30 dias listado em Uso da conta. Na tabela abaixo da coluna Custo projetado, selecione um valor para visualizar um detalhamento do uso por tipo de escaneamento dessa conta. Nesse painel de detalhes, você também poderá visualizar quais tipos de escaneamento têm um teste gratuito ativo para essa conta.

Se você for o administrador delegado de uma organização, visualizará uma linha na tabela para cada conta dentro da sua organização. Se uma conta em sua organização for desassociada, o console mostrará seu custo projetado como um -.

Na guia Por tipo de verificação, visualize um detalhamento do uso real até o momento no período atual de 30 dias por tipo de verificação. Essas são as informações usadas para calcular os custos projetados na guia Por conta.

Se você for o administrador delegado de uma organização, poderá visualizar o uso de cada conta em sua organização.

Nessa guia, você poderá expandir qualquer um dos seguintes painéis para obter estatísticas de uso:

Verificar o Amazon EC2

O console de uso do Amazon Inspector rastreia as seguintes métricas para escaneamento baseado em agente e escaneamento sem agente:

- Instâncias (Média): o Amazon Inspector usa as horas de cobertura para calcular o número médio de recursos para a verificação de instâncias do EC2. A média é o total de horas de cobertura dividido por 720 horas (o número de horas em um período de 30 dias).
- Horas de cobertura: para a verificação do Amazon EC2, esse é o número total de horas nos últimos 30 dias em que o Amazon do Amazon Inspector forneceu cobertura ativa para cada instância do EC2 em uma conta. Para instâncias EC2, as horas de cobertura são as horas a partir do momento em que o Amazon Inspector descobriu a instância até que ela seja encerrada, interrompida ou excluída das verificações por tags. Ao reiniciar uma instância parada ou remover uma tag de exclusão, o Amazon Inspector retoma a cobertura e as horas de cobertura dessa instância continuarão sendo acumuladas.

Escaneamentos de instância do CIS — O número total de escaneamentos do CIS realizados para instâncias na conta.

Escaneamento do Amazon ECR

Verificações iniciais: a soma total das primeiras verificações de imagens na conta nos últimos 30 dias.

Novas verificações: a soma total das novas verificações de imagens na conta nos últimos 30 dias. Uma nova verificação é qualquer verificação feita em uma imagem do ECR que o Amazon Inspector tenha verificado anteriormente. Se configurou seu repositório do ECR para verificação contínua, as novas verificações ocorrem automaticamente quando o Amazon Inspector adiciona uma nova CVE (vulnerabilidades e exposições comuns) ao seu banco de dados.

Verificação do Lambda

O console de uso do Amazon Inspector rastreia as seguintes métricas para escaneamento padrão Lambda e escaneamento de código Lambda:

- Número de funções do Lambda (Avg) — O Amazon Inspector usa as horas de cobertura para calcular o número médio de funções para a verificação da função Lambda. A média é o total de horas de cobertura dividido por 720 horas (o número de horas em um período de 30 dias).
- Horas de cobertura: para a verificação da função do Lambda, esse é o número total de horas nos últimos 30 dias em que o Amazon Inspector forneceu cobertura ativa para cada função do Lambda em uma conta. Para funções do AWS Lambda , as horas de cobertura são calculadas a partir do momento em que o Amazon Inspector descobre uma função até quando ela é

excluída ou excluída das verificações. Se uma função excluída for incluída novamente, as horas de cobertura dessa função continuarão sendo acumuladas.

# Entendendo como o Amazon Inspector calcula os custos de uso

Os custos fornecidos pelo Amazon Inspector são estimativas, não custos reais, portanto, eles podem ser diferentes dos do seu AWS Billing console.

Observe o seguinte sobre como o Amazon Inspector calcula o custo na página de Uso:

- O custo de uso reflete somente a região atual. Os preços por tipo de digitalização variam de acordo com a AWS região. Para verificar os preços exatos por região, consulte os preços do Amazon Inspector
- Todas as projeções de uso são arredondadas para o dólar americano mais próximo.
- Os descontos não estão incluídos nos custos projetados.
- O custo projetado representa o custo total do período de uso de 30 dias por tipo de verificação. Se uma conta tiver menos de 30 dias de uso, o Amazon Inspector projetará o custo após 30 dias, como se algum recurso atualmente coberto permanecesse coberto pelo resto do período de 30 dias.
- O custo por tipo de verificação é calculado com base no seguinte:
  - Verificação do EC2: o custo reflete o número médio de instâncias EC2 cobertas pelo Amazon Inspector nos últimos 30 dias.
  - Verificação de contêineres ECR: o custo reflete a soma do número de verificações iniciais de imagens e novas verificações de imagem nos últimos 30 dias.
  - Escaneamento padrão do Lambda: o custo reflete o número médio de funções do Lambda cobertas pelo Amazon Inspector nos últimos 30 dias.
  - Escaneamento de código do Lambda: o custo reflete o número médio de funções do Lambda cobertas pelo Amazon Inspector nos últimos 30 dias.

# Sobre o teste gratuito do Amazon Inspector

Ao ativar um tipo de verificação do Amazon Inspector, você é automaticamente inscrito em um teste gratuito de 15 dias para esse tipo de verificação. Cada tipo de verificação tem uma trilha gratuita independente, que inclui: escaneamento do EC2, escaneamento do ECR, escaneamento padrão do Lambda e escaneamento de código do Lambda.

> **Note**
>
> O teste gratuito não se aplica ao escaneamento do CIS.

Se desativar um tipo de verificação durante o teste gratuito, o teste gratuito será pausado para esse tipo de verificação. Se reativar esse serviço, o teste gratuito será retomado e você receberá os dias restantes desse teste gratuito.

# Segurança no Amazon Inspector

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

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

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

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

Tópicos

# Proteção de dados no Amazon Inspector

O modelo de responsabilidade AWS compartilhada se aplica à proteção de dados no Amazon Inspector. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a AWS postagem do blog Shared Responsibility Model and GDPR no AWS Blog de segurança da.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de email dos seus clientes, em marcações ou campos de formato livre, como um campo Name (Nome). Isso inclui quando você trabalha com o Amazon Inspector ou outro Serviços da AWS usando o console, a API ou AWS os AWS CLI SDKs. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou

de diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Tópicos



## Criptografia em repouso

O Amazon Inspector armazena com segurança seus dados em repouso usando soluções de AWS criptografia por padrão. O Amazon Inspector criptografa dados, como inventário de recursos coletados usando o AWS Systems Manager, inventário de recursos analisado a partir de imagens do Amazon ECR e descobertas de segurança geradas, AWS usando chaves de criptografia próprias AWS do Key Management Service ().AWS KMS Você não pode visualizar, gerenciar ou usar chaves AWS próprias nem auditar seu uso. No entanto, você não precisa fazer nada e nem alterar qualquer programa para proteger as chaves que criptografam seus dados. Para obter mais informações, consulte chaves do AWS.

Se desativar o Amazon Inspector, ele excluirá permanentemente todos os recursos que ele armazena ou mantém para você, como inventário coletado e descobertas de segurança.

### Criptografia em repouso para código em suas descobertas

Para a digitalização de código Lambda do Amazon Inspector, o Amazon Inspector faz parceria CodeGuru para escanear seu código em busca de vulnerabilidades. Quando uma vulnerabilidade é detectada, CodeGuru extrai um trecho do seu código contendo a vulnerabilidade e armazena esse código até que o Amazon Inspector solicite acesso. Por padrão, CodeGuru usa uma chave AWS própria para criptografar o código extraído, no entanto, você pode configurar o Amazon Inspector para usar sua própria chave AWS KMS gerenciada pelo cliente para criptografia.

O fluxo de trabalho a seguir explica como o Amazon Inspector usa a chave que você configura para criptografar o código:

1. Você fornece uma AWS KMS chave para o Amazon Inspector usando a API do Amazon UpdateEncryptionKeyInspector.
2. O Amazon Inspector encaminha as informações sobre sua AWS KMS chave para. CodeGuru CodeGuru armazena as informações para uso futuro.

3. CodeGuru solicita uma concessão AWS KMS para a chave que você configurou no Amazon Inspector.
4. CodeGuru cria uma chave de dados criptografada a partir da sua AWS KMS chave e a armazena. Essa chave de dados é usada para criptografar seus dados de código armazenados pelo CodeGuru.
5. Sempre que o Amazon Inspector solicita dados de escaneamentos de código, CodeGuru usa a concessão para descriptografar a chave de dados criptografada e, em seguida, usa essa chave para descriptografar os dados para que possam ser recuperados.

Quando você desativa a digitalização de código Lambda, CodeGuru retira a concessão e exclui a chave de dados associada.

### É possível usar uma chave gerenciada pelo cliente para criptografar um volume.

Para usar a criptografia, você precisa ter uma política que permita o acesso às AWS KMS ações, bem como uma declaração que conceda ao Amazon Inspector e CodeGuru permissões para usar essas ações por meio de chaves de condição.

Se estiver configurando, atualizando ou redefinindo a chave de criptografia da conta, precisará usar uma política de administrador do Amazon Inspector, como AWS política gerenciada: AmazonInspector2FullAccess. Você também precisará conceder as seguintes permissões aos usuários somente para leitura que precisam recuperar trechos de código de descobertas ou dados sobre a chave escolhida para criptografia.

Para o KMS, a política deve permitir executar as seguintes ações:

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKeyWithoutPlainText`
- `kms:Encrypt`
- `kms:RetireGrant`

Depois de verificar se você tem as AWS KMS permissões corretas em sua política, você deve anexar uma declaração que permita que o Amazon Inspector use sua chave para criptografia. CodeGuru Anexe a seguinte declaração de política:

> **Note**
>
> Substitua a região pela AWS região na qual você habilitou a digitalização de código do Amazon Inspector Lambda.

```
{
            "Sid": "allow CodeGuru Security to request a grant for a AWS KMS key",
          "Effect": "Allow",
          "Action": "kms:CreateGrant",
          "Resource": "*",
          "Condition": {
           "ForAllValues:StringEquals": {
            "kms:GrantOperations": [
             "GenerateDataKey",
             "GenerateDataKeyWithoutPlaintext",
             "Encrypt",
             "Decrypt",
             "RetireGrant",
             "DescribeKey"
            ]
           },
           "StringEquals": {
            "kms:ViaService": [
             "codeguru-security.Region.amazonaws.com"
            ]
           }
          }
         },
         {
          "Sid": "allow Amazon Inspector and CodeGuru Security to use your AWS KMS key",
          "Effect": "Allow",
          "Action": [
           "kms:Encrypt",
           "kms:Decrypt",
           "kms:RetireGrant",
           "kms:DescribeKey",
           "kms:GenerateDataKeyWithoutPlaintext"
          ],
          "Resource": "*",
          "Condition": {
```

```
          "StringEquals": {
           "kms:ViaService": [
            "inspector2.Region.amazonaws.com",
            "codeguru-security.Region.amazonaws.com"
           ]
          }
         }
        }
```

> **Note**
>
> Ao adicionar a instrução, verifique se a sintaxe é válida. As políticas usam o formato JSON. Isso significa que você precisa adicionar uma vírgula antes ou depois da declaração, dependendo de onde você adiciona a declaração à política. Se você incluir a instrução como a última instrução, adicione uma vírgula após o colchete de fechamento para a instrução anterior. Se você adicioná-la como a primeira instrução ou adicioná-la entre duas instruções existentes, adicione uma vírgula após o colchete de fechamento.

### É possível usar uma chave gerenciada pelo cliente para criptografar um volume.

Para configurar a criptografia para sua conta usando uma chave gerenciada pelo cliente, você deve ser um administrador do Amazon Inspector com as permissões descritas em É possível usar uma chave gerenciada pelo cliente para criptografar um volume.. Além disso, você precisará de uma AWS KMS chave na mesma AWS região de suas descobertas ou de uma chave multirregional. Você pode usar uma chave simétrica existente em sua conta ou criar uma chave simétrica gerenciada pelo cliente usando o AWS Management Console ou as AWS KMS APIs. Para obter mais informações, consulte Criação de AWS KMS chaves de criptografia simétricas no guia do AWS KMS usuário.

Usando a API do Amazon Inspector para configurar a criptografia

Para definir uma chave para criptografia, a UpdateEncryptionKeyoperação da API do Amazon Inspector enquanto estiver conectado como administrador do Amazon Inspector. Na solicitação da API, use o `kmsKeyId` campo para especificar o ARN da AWS KMS chave que você deseja usar. Para `scanType` digitar o `CODE` e para `resourceType` digitar o `AWS_LAMBDA_FUNCTION`.

Você pode usar a UpdateEncryptionKeyAPI para verificar qual AWS KMS chave o Amazon Inspector está usando para criptografia.

> **Note**
>
> Se você tentar `GetEncryptionKey` usar sem definir uma chave gerenciada pelo cliente, a operação retornará um `ResourceNotFoundException` erro, o que significa que uma AWS chave própria está sendo usada para criptografia.

Se você excluir ou alterar a chave ou alterar sua política para negar acesso ao Amazon Inspector ou CodeGuru não conseguir acessar suas descobertas de vulnerabilidade de código, a digitalização de código Lambda falhará em sua conta.

Você pode usar `ResetEncryptionKey` para continuar usando uma chave AWS própria para criptografar o código extraído como parte das descobertas do Amazon Inspector.

### Criptografia em trânsito

AWS criptografa todos os dados em trânsito entre sistemas AWS internos e outros AWS serviços.

Para coleta de inventário, o Systems Manager reúne dados de telemetria de instâncias EC2 de propriedade do cliente que ele envia de volta por meio de um canal protegido pelo Transport Layer Security (TLS) para AWS avaliação. Consulte Proteção de dados no Systems Manager para entender como o SSM criptografa dados em trânsito.

Da mesma forma, as descobertas de escaneamento de funções do Amazon ECR e AWS do Lambda enviadas ao Security Hub são criptografadas usando um canal protegido por TLS.

## Identity and Access Management para o Amazon Inspector

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (ter permissões) para usar os recursos do Amazon Inspector. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Público
- Autenticando com identidades

- Gerenciando acesso usando políticas
- Como o Amazon Inspector funciona com o IAM
- Exemplos de políticas baseadas em identidade para o Amazon Inspector
- AWS políticas gerenciadas para o Amazon Inspector
- Uso de funções vinculadas a serviço para o Amazon Inspector
- Solução de problemas de identidade e acesso do Amazon Inspector

## Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Amazon Inspector.

Usuário do serviço: se você usar o serviço do Amazon Inspector para fazer seu trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que mais recursos do Amazon Inspector forem usados para realizar o trabalho, talvez sejam necessárias permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não puder acessar um recurso no Amazon Inspector, consulte Solução de problemas de identidade e acesso do Amazon Inspector.

Administrador do serviço: se você for o responsável pelos recursos do Amazon Inspector na sua empresa, provavelmente terá acesso total ao Amazon Inspector. Cabe a você determinar que funcionalidades e recursos do Amazon Inspector os usuários do seu serviço devem acessar. Assim, é necessário enviar solicitações ao administrador do IAM para alterar as permissões dos usuários do seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como a empresa pode usar o IAM com o Amazon Inspector, consulte Como o Amazon Inspector funciona com o IAM.

Administrador do IAM: se você for um administrador do IAM, talvez queira saber detalhes sobre como emitir políticas para gerenciar o acesso ao Amazon Inspector. Para visualizar exemplos de políticas baseadas em identidade do Amazon Inspector que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade para o Amazon Inspector.

## Autenticando com identidades

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

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

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

### Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM.

### Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o . AWS IAM Identity Center Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no AWS IAM Identity Center Manual do Usuário do.

## Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, 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

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de

funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para 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 Center Manual 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.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões

para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

- Função de Serviço: uma função de serviço é 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 ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas a serviço.

- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para 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 AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão Geral das Políticas JSON no Guia do Usuário do IAM.

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

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM às 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 função da AWS Management Console AWS CLI, da ou da AWS API.

### Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do 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. 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 autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como 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 recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de função do IAM e as políticas 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. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

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

## Listas de controle de acesso (ACLs)

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

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF 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

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade e dos seus limites de permissões. As políticas baseadas em atributo que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de Permissões para 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 (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte Como os SCPs Funcionam no AWS Organizations Manual 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 atributo. Uma negação explícita em qualquer uma dessas políticas

substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

### Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

## Como o Amazon Inspector funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Amazon Inspector, entenda quais são os atributos do IAM que estão disponíveis para uso com o Amazon Inspector.

Recursos do IAM que você pode usar com o Amazon Inspector

| Atributo do IAM | Suporte do Amazon Inspector |
|---|---|
| Políticas baseadas em identidade | Sim |
| Políticas baseadas em recursos | Não |
| Ações das políticas | Sim |
| atributos de políticas | Sim |
| Chaves de condição de política (específicas do serviço) | Sim |
| ACLs | Não |
| ABAC (tags em políticas) | Parcial |
| Credenciais temporárias | Sim |
| Permissões de entidade principal | Sim |
| Perfis de serviço | Não |

| Atributo do IAM | Suporte do Amazon Inspector |
| --- | --- |
| Funções vinculadas ao serviço | Sim |

Para obter uma visão de alto nível de como o Amazon Inspector e Serviços da AWS outros funcionam com a maioria dos recursos do IAM, Serviços da AWS veja esse trabalho com o IAM no Guia do usuário do IAM.

## Políticas baseadas em identidade do Amazon Inspector

| | |
| --- | --- |
| 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. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade para o Amazon Inspector

Para ver exemplos de políticas baseadas em identidade do Amazon Inspector, consulte Exemplos de políticas baseadas em identidade para o Amazon Inspector.

## Políticas baseadas em recursos no Amazon Inspector

| | |
| --- | --- |
| Oferece suporte a políticas baseadas em recursos | Não |

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de função do IAM e as políticas 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. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em atributo é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em atributo conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

## Ações de políticas para o Amazon Inspector

| | |
|---|---|
| Oferece suporte a ações de políticas | Sim |

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

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações do Amazon Inspector, consulte Ações definidas pelo Amazon Inspector na Referência de autorização do serviço.

As ações de políticas no Amazon Inspector usam o seguinte prefixo antes da ação:

```
inspector2
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
      "inspector2:action1",
      "inspector2:action2"
         ]
```

Para ver exemplos de políticas baseadas em identidade do Amazon Inspector, consulte Exemplos de políticas baseadas em identidade para o Amazon Inspector.

## Recursos de política do Amazon Inspector

| | |
|---|---|
| Oferece suporte a atributos de políticas | Sim |

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

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

Para ações não compatíveis com permissões no 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 recursos do Amazon Inspector e seus ARNs, consulte Recursos definidos pelo Amazon Inspector Classic na Referência de autorização do serviço. Para saber com quais ações é possível especificar o ARN de cada recurso, consulte Ações definidas pelo Amazon Inspector.

Para ver exemplos de políticas baseadas em identidade do Amazon Inspector, consulte Exemplos de políticas baseadas em identidade para o Amazon Inspector.

## Chaves de condição de políticas do Amazon Inspector.

| | |
|---|---|
| Suporta chaves de condição de política específicas de serviço | Sim |

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual 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 `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos de Política do IAM: Variáveis e Tags no Guia do Usuário do IAM.

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

Para ver uma lista de chaves de condição do Amazon Inspector, consulte Chaves de condição do Amazon Inspector na Referência de autorização do serviço. Para saber com quais ações e recursos é possível usar a chave de condição, consulte Ações definidas pelo Amazon Inspector.

Para ver exemplos de políticas baseadas em identidade do Amazon Inspector, consulte Exemplos de políticas baseadas em identidade para o Amazon Inspector.

## ACLs no Amazon Inspector

| | |
|---|---|
| Oferece suporte a ACLs | Não |

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

## ABAC com o Amazon Inspector

| | |
|---|---|
| Oferece suporte a ABAC (tags em políticas) | Parcial |

O controle de acesso baseado em recurso (ABAC) é uma estratégia de autorização que define permissões com base em recursos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do 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 todo 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 por atributo (ABAC) no Guia do usuário do IAM.

## Usar credenciais temporárias com o Amazon Inspector

| | |
|---|---|
| Oferece suporte a credenciais temporárias | Sim |

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS trabalhar com o IAM no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para uma Função (Console) no Guia do Usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte Credenciais de segurança temporárias no IAM.

## Permissões de entidades principais entre serviços para o Amazon Inspector

| | |
|---|---|
| Suporte para o recurso Encaminhamento de sessões de acesso (FAS) | Sim |

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

## Perfis de serviço do Amazon Inspector

| | |
|---|---|
| Oferece suporte a perfis de serviço | Não |

O perfil de serviço é um perfil do IAMhttps://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html 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.

> **Warning**
>
> Mudar as permissões para um perfil de serviço pode interromper a funcionalidade do Amazon Inspector. Edite perfis de serviço somente quando o Amazon Inspector fornecer orientação para isso.

### Perfis vinculados a serviço do Amazon Inspector

| | |
|---|---|
| Oferece suporte a perfis vinculados ao serviço | Sim |

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um 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 vinculadas a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado ao serviço desse serviço.

## Exemplos de políticas baseadas em identidade para o Amazon Inspector

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do Amazon Inspector. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. 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 aos perfis, e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo Amazon Inspector, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para o Amazon Inspector na Referência de autorização do serviço.

Tópicos

- Melhores práticas de política
- Usar o console do Amazon Inspector
- Permitir que usuários visualizem suas próprias permissões
- Permitir acesso somente leitura a todos os recursos do Amazon Inspector
- Permitir acesso total a todos os recursos do Amazon Inspector

## Melhores práticas de política

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

- Comece com políticas AWS gerenciadas e avance para permissões de privilégios mínimos — Para começar a conceder permissões para seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas Gerenciadas pela AWS ou 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 atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e Permissões no IAM no Guia do Usuário do IAM.
- 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 às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS

CloudFormation. Para obter mais informações, consulte 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 você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir 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.

## Usar o console do Amazon Inspector

Para acessar o console do Amazon Inspector, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e veja detalhes sobre os recursos do Amazon Inspector em sua Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o console do Amazon Inspector, anexe também o Amazon `ConsoleAccess` Inspector `ReadOnly` AWS ou a política gerenciada às entidades. Para obter mais informações, consulte Adicionando Permissões a um Usuário no Guia do Usuário do IAM.

## 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 programaticamente usando a API AWS CLI ou AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

## Permitir acesso somente leitura a todos os recursos do Amazon Inspector

Este exemplo exibe uma política que permite acesso somente de leitura a todos os recursos do Amazon Inspector.

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "inspector2:Describe*",
                "inspector2:Get*",
                "inspector2:BatchGet*",
                "inspector2:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

## Permitir acesso total a todos os recursos do Amazon Inspector

Este exemplo exibe uma política que permite acesso total a todos os recursos do Amazon Inspector.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "inspector2:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
```

```
                    "iam:AWSServiceName": "inspector2.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

## AWS políticas gerenciadas para o Amazon Inspector

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

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

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

## AWS política gerenciada: AmazonInspector2FullAccess

É possível anexar a política `AmazonInspector2FullAccess` a suas identidades do IAM.

Essa política concede permissões administrativas ao Amazon Inspector.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `inspector2`: oferece acesso total à funcionalidade do Amazon Inspector.
- `iam`: permite que o Amazon Inspector crie a função vinculada ao serviço`AmazonInspector2AgentlessServiceRole`. Isso é necessário para que o Amazon Inspector possa realizar operações como recuperar informações sobre as instâncias do Amazon EC2 e repositórios e imagens de contêineres do Amazon ECR, analisar a rede VPC e descrever contas associadas à sua organização. Para ter mais informações, consulte Uso de funções vinculadas a serviço para o Amazon Inspector.
- `organizations`: permite que os administradores usem o Amazon Inspector para uma organização no AWS Organizations. Depois de ativar o acesso confiável para o Amazon Inspector AWS Organizations em, os membros da conta de administrador delegado podem gerenciar configurações e visualizar descobertas em toda a organização.
- `codeguru-security`— Permite que os administradores usem o Amazon Inspector para recuperar trechos de código de informações e alterar as configurações de criptografia do código armazenado pela Security. CodeGuru Para ter mais informações, consulte Criptografia em repouso para código em suas descobertas.

```
{
```

```
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "inspector2:*",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "codeguru-security:BatchGetFindings",
    "codeguru-security:GetAccountConfiguration",
    "codeguru-security:UpdateAccountConfiguration"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "iam:CreateServiceLinkedRole",
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "iam:AWSServiceName": "inspector2.amazonaws.com"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": [
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization"
   ],
   "Resource": "*"
  }
 ]
}
```

## AWS política gerenciada: AmazonInspector2ReadOnlyAccess

É possível anexar a política `AmazonInspector2ReadOnlyAccess` a suas identidades do IAM.

Essa política concede permissões de acesso somente leitura ao Amazon Inspector.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `inspector2`: oferece acesso somente de leitura à funcionalidade do Amazon Inspector.
- `organizations`— Permite que detalhes sobre a cobertura do Amazon Inspector para uma organização sejam AWS Organizations visualizados.
- `codeguru-security`— Permite que trechos de código sejam recuperados da Segurança. CodeGuru Também permite que as configurações de criptografia do seu código armazenado em CodeGuru Segurança sejam visualizadas.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "inspector2:BatchGet*",
    "inspector2:List*",
    "inspector2:Describe*",
    "inspector2:Get*",
    "inspector2:Search*",
    "codeguru-security:BatchGetFindings",
    "codeguru-security:GetAccountConfiguration"
   ],
   "Resource": "*"
  }
 ]
}
```

## AWS política gerenciada: AmazonInspector2ManagedCisPolicy

Também é possível anexar a política `AmazonInspector2ManagedCisPolicy` às suas entidades do IAM. Essa política deve ser anexada a uma função que conceda permissões às suas instâncias do Amazon EC2 para executar escaneamentos CIS da instância. Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo solicitações AWS CLI de AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para 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.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `inspector2`— Permite acesso às ações usadas para executar varreduras do CIS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
            "inspector2:StartCisSession",
            "inspector2:StopCisSession",
            "inspector2:SendCisSessionTelemetry",
            "inspector2:SendCisSessionHealth"
            ],
            "Resource": "*",
        }
     ]
 }
```

## AWS política gerenciada: AmazonInspector2ServiceRolePolicy

Não é possível anexar a política `AmazonInspector2ServiceRolePolicy` às suas entidades do IAM. Essa política é anexada a uma função vinculada ao serviço que permite que o Amazon

Inspector realize ações em seu nome. Para ter mais informações, consulte Uso de funções vinculadas a serviço para o Amazon Inspector.

### AWS política gerenciada: AmazonInspector2AgentlessServiceRolePolicy

Não é possível anexar a política `AmazonInspector2AgentlessServiceRolePolicy` às suas entidades do IAM. Essa política é anexada a uma função vinculada ao serviço que permite que o Amazon Inspector realize ações em seu nome. Para ter mais informações, consulte Uso de funções vinculadas a serviço para o Amazon Inspector.

## Atualizações do Amazon Inspector para AWS políticas gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Amazon Inspector desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre mudanças nesta página, assine o feed RSS na página Histórico de documentos do Amazon Inspector.

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonInspector2 ManagedCisPolicy — Nova política | O Amazon Inspector adicionou uma nova política gerenciada que você pode usar como parte de um perfil de instância para permitir escaneamentos do CIS em uma instância. | 23 de janeiro de 2024 |
| AmazonInspector2 ServiceRolePolicy — Atualizações em uma política existente | O Amazon Inspector adicionou novas permissões que permitem que o Amazon Inspector inicie escaneamentos do CIS nas instâncias de destino. | 23 de janeiro de 2024 |
| AmazonInspector2 AgentlessServiceRolePolicy — Nova política | O Amazon Inspector adicionou uma nova política de função vinculada ao serviço para | 27 de novembro de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| | permitir a verificação sem agente da instância do EC2. | |
| AmazonInspector2 ReadOnlyAccess — Atualizações em uma política existente | O Amazon Inspector adicionou novas permissões que permitem que usuários somente de leitura recuperem detalhes de inteligência de vulnerabilidade para descobertas de vulnerabilidades de pacotes. | 22 de setembro de 2023 |
| AmazonInspector2 ServiceRolePolicy — Atualizações em uma política existente | O Amazon Inspector adicionou novas permissões que permitem que o Amazon Inspector verifique as configurações de rede das instâncias do Amazon EC2 que fazem parte dos grupos-alvo do Elastic Load Balancing. | 31 de agosto de 2023 |
| AmazonInspector2 ReadOnlyAccess — Atualizações em uma política existente | O Amazon Inspector adicionou novas permissões que permitem que usuários somente para leitura exportem a SBOM (Lista de Materiais de Software) para seus recursos. | 29 de junho de 2023 |
| AmazonInspector2 ReadOnlyAccess — Atualizações em uma política existente | O Amazon Inspector adicionou novas permissões que permitem que usuários somente de leitura recuperem detalhes das configurações de criptografia das descobertas da digitalização de código Lambda em suas contas. | 13 de junho de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonInspector2 FullAccess — Atualizações em uma política existente | O Amazon Inspector adicionou novas permissões que permitem aos usuários configurar uma chave KMS gerenciada pelo cliente para criptografar o código nas descobertas da digitalização de código Lambda. | 13 de junho de 2023 |
| AmazonInspector2 ReadOnlyAccess — Atualizações em uma política existente | O Amazon Inspector adicionou novas permissões que permitem que usuários somente de leitura recuperem detalhes do status e descobertas da verificação de código Lambda para sua conta. | 2 de maio de 2023 |
| AmazonInspector2 ServiceRolePolicy — Atualizações em uma política existente | O Amazon Inspector adicionou novas permissões que permitem que o Amazon Inspector AWS CloudTrail crie canais vinculados a serviços em sua conta quando você ativa a digitalização Lambda. Isso permite que o Amazon Inspector monitore CloudTrail eventos em sua conta. | 30 de abril de 2023 |
| AmazonInspector2 FullAccess — Atualizações em uma política existente | O Amazon Inspector adicionou novas permissões que permitem que usuários recuperem detalhes de descobertas de vulnerabilidade de código da verificação de código Lambda. | 21 de abril de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonInspector2 ServiceRolePolicy — Atualizações em uma política existente | O Amazon Inspector adicionou novas permissões que permitem que o Amazon Inspector envie informaçõ es ao Amazon EC2 Systems Manager sobre os caminhos personalizados que um cliente definiu para a inspeção profunda do Amazon EC2. | 17 de abril de 2023 |
| AmazonInspector2 ServiceRolePolicy — Atualizações em uma política existente | O Amazon Inspector adicionou novas permissões que permitem que o Amazon Inspector AWS CloudTrail crie canais vinculados a serviços em sua conta quando você ativa a digitalização Lambda. Isso permite que o Amazon Inspector monitore CloudTrail eventos em sua conta. | 30 de abril de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonInspector2 ServiceRolePolicy — Atualizações em uma política existente | O Amazon Inspector adicionou novas permissões que permitem que o Amazon Inspector solicite escaneamentos do código do desenvolvedor AWS Lambda em funções e receba dados de escaneamento da Amazon Security. CodeGuru Além disso, o Amazon Inspector adicionou permissões para examinar as políticas do IAM. O Amazon Inspector usa essas informações para verificar as vulnerabilidades do código nas funções do Lambda. | 28 de fevereiro de 2023 |
| AmazonInspector2 ServiceRolePolicy — Atualizações em uma política existente | O Amazon Inspector adicionou uma nova declaração que permite ao Amazon Inspector recuperar informações sobre quando AWS Lambda uma função foi invocada CloudWatch pela última vez. O Amazon Inspector usa essas informações para focar as varreduras nas funções do lambda em seu ambiente que estiveram ativas nos últimos 90 dias. | 20 de fevereiro de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonInspector2 ServiceRolePolicy — Atualizações em uma política existente | O Amazon Inspector adicionou uma nova declaração que permite ao Amazon Inspector recuperar informações AWS Lambda sobre funções, incluindo cada versão de camada associada a cada função. O Amazon Inspector usa essas informações para verificar se há vulnerabilidades de segurança nas funções do Lambda. | 28 de novembro de 2022 |
| AmazonInspector2 ServiceRolePolicy — Atualizações em uma política existente | O Amazon Inspector adicionou uma nova ação para permitir que o Amazon Inspector descreva execuções de associação do SSM. Além disso, o Amazon Inspector também adicionou um escopo adicional de recursos para permitir que o Amazon Inspector crie, atualize, exclua e inicie associações do SSM com documentos do SSM de propriedade do `AmazonInspector2` . | 31 de agosto de 2022 |
| AmazonInspector2 ServiceRolePolicy Atualizações em uma política existente | O Amazon Inspector atualizou o escopo dos recursos da política para permitir que o Amazon Inspector colete inventário de software em outras partições. AWS | 12 de agosto de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonInspector2 ServiceRolePolicy — Atualizações em uma política existente | O Amazon Inspector estruturou novamente o escopo dos recursos das ações, permitindo que o Amazon Inspector crie, exclua e atualize associações de SSM. | 10 de agosto de 2022 |
| AmazonInspector2 ReadOnlyAccess — Nova política | O Amazon Inspector adicionou uma nova política para permitir acesso somente leitura à funcionalidade do Amazon Inspector. | 21 de janeiro de 2022 |
| AmazonInspector2 FullAccess — Nova política | O Amazon Inspector adicionou uma nova política para permitir acesso total à funcionalidade do Amazon Inspector. | 29 de novembro de 2021 |
| AmazonInspector2 ServiceRolePolicy — Nova política | O Amazon Inspector adicionou uma nova política para permitir que o Amazon Inspector execute ações em outros serviços em seu nome. | 29 de novembro de 2021 |
| O Amazon Inspector passou a monitorar alterações | O Amazon Inspector começou a rastrear alterações em suas políticas AWS gerenciadas. | 29 de novembro de 2021 |

## Uso de funções vinculadas a serviço para o Amazon Inspector

O Amazon Inspector usa uma função vinculada ao serviço AWS Identity and Access Management (IAM) chamada. `AWSServiceRoleForAmazonInspector2` Perfil vinculado a serviço é um tipo especial de perfil do IAM que é vinculado diretamente ao Amazon Inspector. É predefinido pelo

Amazon Inspector e inclui todas as permissões que o Amazon Inspector exige para ligar Serviços da AWS para outras pessoas em seu nome.

O perfil vinculado a serviço facilita a configuração do Amazon Inspector porque você não precisa adicionar as permissões necessárias manualmente. O Amazon Inspector define as permissões dos perfis vinculados a serviço e, exceto se definido de outra forma, somente o Amazon Inspector pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

É necessário configurar permissões para que uma entidade do IAM (por exemplo, um grupo ou perfil) crie, edite ou exclua um perfil vinculado a serviço. Para obter mais informações, consulte Permissões de perfil vinculado a serviços no Guia do usuário do IAM. Você pode excluir uma função vinculada ao serviço somente depois de excluir seus recursos relacionados. Isso protege seus recursos do Amazon Inspector, pois você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com perfis vinculados ao serviço, consulte serviços da AWS que funcionam com o IAM e procure os serviços que apresentam Sim na coluna Perfis vinculados aos serviços. Escolha um Sim com um link para revisar a documentação da função vinculada a esse serviço.

## Permissões de perfil vinculado a serviço para o Amazon Inspector.

O Amazon Inspector usa o perfil vinculado a serviço chamado `AWSServiceRoleForAmazonInspector2`. Essa função vinculada a serviço confia no serviço `inspector2.amazonaws.com` para assumir a função.

A política de permissões para a função, que é chamda de `AmazonInspector2ServiceRolePolicy`, permite que o Amazon Inspector execute tarefas como:

- Use ações do Amazon Elastic Compute Cloud (Amazon EC2) para recuperar informações sobre instâncias e caminhos de rede.
- Use AWS Systems Manager ações para recuperar o inventário de suas instâncias do Amazon EC2 e para recuperar informações sobre pacotes de terceiros a partir de caminhos personalizados.
- Use a AWS Systems Manager `SendCommand` ação para invocar escaneamentos do CIS para instâncias de destino.
- Use as ações do Amazon Elastic Container Registry para recuperar informações sobre suas imagens de contêiner.
- Use AWS Lambda ações para recuperar informações sobre suas funções do Lambda.

- Use AWS Organizations ações para descrever contas associadas.
- Use CloudWatch ações para recuperar informações sobre a última vez em que suas funções do Lambda foram invocadas.
- Use ações selecionadas do IAM para recuperar informações sobre as políticas do IAM que poderiam criar vulnerabilidades de segurança no código do Lambda.
- Use ações CodeGuru de segurança para realizar escaneamentos do código em suas funções do Lambda. O Amazon Inspector usa as seguintes ações de CodeGuru segurança:
  - codeguru-security: CreateScan — Concede permissão para criar uma verificação de segurança. CodeGuru
  - codeguru-security: GetScan — Concede permissão para recuperar CodeGuru metadados do Security Scan.
  - codeguru-security: ListFindings — Concede permissão para recuperar descobertas geradas pela Security. CodeGuru
  - codeguru-security: DeleteScansByCategory — Concede permissão para a Segurança excluir escaneamentos CodeGuru iniciados pelo Amazon Inspector.
  - codeguru-security: BatchGetFindings — Concede permissão para recuperar um lote de descobertas específicas geradas pela Security. CodeGuru
- Use ações selecionadas do Elastic Load Balancing para realizar varreduras de rede de instâncias do EC2 que fazem parte dos grupos-alvo do Elastic Load Balancing.

A função está configurada com a seguinte política de permissões:

```
    {
"Version": "2012-10-17",
"Statement": [
 {
  "Sid": "TirosPolicy",
  "Effect": "Allow",
  "Action": [
   "directconnect:DescribeConnections",
   "directconnect:DescribeDirectConnectGatewayAssociations",
   "directconnect:DescribeDirectConnectGatewayAttachments",
   "directconnect:DescribeDirectConnectGateways",
   "directconnect:DescribeVirtualGateways",
   "directconnect:DescribeVirtualInterfaces",
   "ec2:DescribeAvailabilityZones",
```

```
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeManagedPrefixLists",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribePrefixLists",
    "ec2:DescribeRegions",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGatewayConnects",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetManagedPrefixListEntries",
    "ec2:GetTransitGatewayRouteTablePropagations",
    "ec2:SearchTransitGatewayRoutes",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeTargetHealth",
    "network-firewall:DescribeFirewall",
    "network-firewall:DescribeFirewallPolicy",
    "network-firewall:DescribeResourcePolicy",
    "network-firewall:DescribeRuleGroup",
    "network-firewall:ListFirewallPolicies",
    "network-firewall:ListFirewalls",
    "network-firewall:ListRuleGroups",
    "tiros:CreateQuery",
    "tiros:GetQueryAnswer"
```

```
    ],
    "Resource": [
     "*"
    ]
   },
   {
    "Sid": "PackageVulnerabilityScanning",
    "Effect": "Allow",
    "Action": [
     "ecr:BatchGetImage",
     "ecr:BatchGetRepositoryScanningConfiguration",
     "ecr:DescribeImages",
     "ecr:DescribeRegistry",
     "ecr:DescribeRepositories",
     "ecr:GetAuthorizationToken",
     "ecr:GetDownloadUrlForLayer",
     "ecr:GetRegistryScanningConfiguration",
     "ecr:ListImages",
     "ecr:PutRegistryScanningConfiguration",
     "organizations:DescribeAccount",
     "organizations:DescribeOrganization",
     "organizations:ListAccounts",
     "ssm:DescribeAssociation",
     "ssm:DescribeAssociationExecutions",
     "ssm:DescribeInstanceInformation",
     "ssm:ListAssociations",
     "ssm:ListResourceDataSync"
    ],
    "Resource": "*"
   },
   {
    "Sid": "LambdaPackageVulnerabilityScanning",
    "Effect": "Allow",
    "Action": [
     "lambda:ListFunctions",
     "lambda:GetFunction",
     "lambda:GetLayerVersion",
     "cloudwatch:GetMetricData"
    ],
    "Resource": "*"
   },
   {
    "Sid": "GatherInventory",
    "Effect": "Allow",
```

```
    "Action": [
     "ssm:CreateAssociation",
     "ssm:StartAssociationsOnce",
     "ssm:DeleteAssociation",
     "ssm:UpdateAssociation"
    ],
    "Resource": [
     "arn:aws:ec2:*:*:instance/*",
     "arn:aws:ssm:*:*:document/AmazonInspector2-*",
     "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
     "arn:aws:ssm:*:*:managed-instance/*",
     "arn:aws:ssm:*:*:association/*"
    ]
   },
   {
    "Sid": "DataSyncCleanup",
    "Effect": "Allow",
    "Action": [
     "ssm:CreateResourceDataSync",
     "ssm:DeleteResourceDataSync"
    ],
    "Resource": [
     "arn:aws:ssm:*:*:resource-data-sync/InspectorResourceDataSync-do-not-delete"
    ]
   },
   {
    "Sid": "ManagedRules",
    "Effect": "Allow",
    "Action": [
     "events:PutRule",
     "events:DeleteRule",
     "events:DescribeRule",
     "events:ListTargetsByRule",
     "events:PutTargets",
     "events:RemoveTargets"
    ],
    "Resource": [
     "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
    ]
   },
   {
    "Sid": "LambdaCodeVulnerabilityScanning",
    "Effect": "Allow",
    "Action": [
```

```
    "codeguru-security:CreateScan",
    "codeguru-security:GetAccountConfiguration",
    "codeguru-security:GetFindings",
    "codeguru-security:GetScan",
    "codeguru-security:ListFindings",
    "codeguru-security:BatchGetFindings",
    "codeguru-security:DeleteScansByCategory"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Sid": "CodeGuruCodeVulnerabilityScanning",
   "Effect": "Allow",
   "Action": [
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:GetPolicy",
    "iam:GetPolicyVersion",
    "iam:ListAttachedRolePolicies",
    "iam:ListPolicies",
    "iam:ListPolicyVersions",
    "iam:ListRolePolicies",
    "lambda:ListVersionsByFunction"
   ],
   "Resource": [
    "*"
   ],
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "codeguru-security.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "Ec2DeepInspection",
   "Effect": "Allow",
   "Action": [
    "ssm:PutParameter",
    "ssm:GetParameters",
    "ssm:DeleteParameter"
```

```
    ],
    "Resource": [
     "arn:aws:ssm:*:*:parameter/inspector-aws/service/inspector-linux-application-paths"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "AllowManagementOfServiceLinkedChannel",
    "Effect": "Allow",
    "Action": [
     "cloudtrail:CreateServiceLinkedChannel",
     "cloudtrail:DeleteServiceLinkedChannel"
    ],
    "Resource": [
     "arn:aws:cloudtrail:*:*:channel/aws-service-channel/inspector2/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "AllowListServiceLinkedChannels",
    "Effect": "Allow",
    "Action": [
     "cloudtrail:ListServiceLinkedChannels"
    ],
    "Resource": [
     "*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "AllowToRunInvokeCisSpecificDocuments",
    "Effect": "Allow",
```

```
    "Action": [
     "ssm:SendCommand",
     "ssm:GetCommandInvocation"
    ],
    "Resource": [
     "arn:aws:ssm:*:*:document/AmazonInspector2-InvokeInspectorSsmPluginCIS"
    ]
   },
   {
    "Sid": "AllowToRunCisCommandsToSpecificResources",
    "Effect": "Allow",
    "Action": [
     "ssm:SendCommand"
    ],
    "Resource": [
     "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "AllowToPutCloudwatchMetricData",
    "Effect": "Allow",
    "Action": [
     "cloudwatch:PutMetricData"
    ],
    "Resource": [
     "*"
    ],
    "Condition": {
     "StringEquals": {
      "cloudwatch:namespace": "AWS/Inspector2"
     }
    }
   }
  ]
}
```

## Criação de um perfil vinculado a serviço para Amazon Inspector

Não é necessário criar manualmente uma função vinculada a serviço. Quando você ativa o Amazon Inspector na AWS Management Console, na ou na AWS API AWS CLI, o Amazon Inspector cria a função vinculada ao serviço para você.

## Editar um perfil vinculado a serviço do Amazon Inspector

O Amazon Inspector não permite que você edite a função vinculada ao serviço do `AWSServiceRoleForAmazonInspector2`. Após a criação da função vinculada a serviços, você não poderá alterar o nome da função, pois várias entidades podem fazer referência à função. No entanto, será possível editar a descrição da função usando o IAM. Para ter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

## Excluir um perfil vinculado a serviço do Amazon Inspector

Se você não precisa mais usar o Amazon Inspector, recomendamos que exclua a função vinculada a serviço do `AWSServiceRoleForAmazonInspector2`. Antes de excluir a função, você deve desativar o Amazon Inspector em Região da AWS cada local em que ela estiver ativada. Quando o Amazon Inspector é desativado, ele não exclui a função para você. Portanto, se você ativar o Amazon Inspector novamente, ele poderá usar a função existente. Dessa forma, você evita ter uma entidade não utilizada que não seja monitorada ou mantida ativamente. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

Se você excluir essa função vinculada ao serviço e precisar criá-la novamente, poderá usar esse mesmo processo para recriar a função em sua conta. Ao ativar o Amazon Inspector, ele cria novamente a função vinculada ao serviço para você.

> **Note**
>
> Se o serviço do Amazon Inspector estiver usando o perfil quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente fazer a operação novamente.

Você pode usar o console do IAM AWS CLI, o ou a AWS API para excluir a função `AWSServiceRoleForAmazonInspector2` vinculada ao serviço. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

## Permissões de perfil vinculadas ao serviço para verificações sem agente do Amazon Inspector

A verificação sem agente do Amazon Inspector usa o perfil vinculado ao serviço chamada `AWSServiceRoleForAmazonInspector2Agentless`. Essa SLR permite que o Amazon Inspector crie um snapshot de volume do Amazon EBS na conta e acesse os dados desse snapshot. Essa função vinculada a serviços confia no serviço `agentless.inspector2.amazonaws.com` para assumir a função.

> **Important**
>
> As instruções neste perfil vinculada ao serviço evitam que o Amazon Inspector execute verificações sem agente em qualquer instância do EC2 que você tenha excluído das verificações usando a tag `InspectorEc2Exclusion`. Além disso, as instruções impedem que o Amazon Inspector acesse dados criptografados de um volume quando a chave KMS usada para criptografá-lo tiver a tag `InspectorEc2Exclusion`. Para ter mais informações, consulte Excluir instâncias das verificações do Amazon Inspector.

A política de permissões para a função, que é chamda de `AmazonInspector2AgentlessServiceRolePolicy`, permite que o Amazon Inspector execute tarefas como:

- Use ações do Amazon Elastic Compute Cloud (Amazon EC2) para recuperar informações sobre instâncias, volumes e snapshots do EC2.
  - Use ações de marcação do Amazon EC2 para marcar snapshots para verificações com a chave de tag `InspectorScan`.
  - Use ações de snapshot do Amazon EC2 para criar snapshots, marcá-los com a chave de tag `InspectorScan` e, em seguida, excluir snapshots de volumes do Amazon EBS que foram marcados com a chave de tag `InspectorScan`.
- Use ações do Amazon EBS para recuperar informações de snapshots marcados com a chave de tag `InspectorScan`.
- Use ações de AWS KMS descriptografia selecionadas para descriptografar instantâneos criptografados com chaves gerenciadas pelo cliente. AWS KMS O Amazon Inspector não descriptografa snapshots quando a chave KMS usada para criptografá-los é marcada com a tag `InspectorEc2Exclusion`.

A função está configurada com a seguinte política de permissões:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "InstanceIdentification",
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeInstances",
    "ec2:DescribeVolumes",
    "ec2:DescribeSnapshots"
   ],
   "Resource": "*"
  },
  {
   "Sid": "GetSnapshotData",
   "Effect": "Allow",
   "Action": [
    "ebs:ListSnapshotBlocks",
    "ebs:GetSnapshotBlock"
   ],
   "Resource": "arn:aws:ec2:*:*:snapshot/*",
   "Condition": {
    "StringLike": {
     "aws:ResourceTag/InspectorScan": "*"
    }
   }
  },
  {
   "Sid": "CreateSnapshotsAnyInstanceOrVolume",
   "Effect": "Allow",
   "Action": "ec2:CreateSnapshots",
   "Resource": [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*"
   ]
  },
  {
   "Sid": "DenyCreateSnapshotsOnExcludedInstances",
   "Effect": "Deny",
   "Action": "ec2:CreateSnapshots",
   "Resource": "arn:aws:ec2:*:*:instance/*",
```

```
    "Condition": {
     "StringEquals": {
      "ec2:ResourceTag/InspectorEc2Exclusion": "true"
     }
    }
   },
   {
    "Sid": "CreateSnapshotsOnAnySnapshotOnlyWithTag",
    "Effect": "Allow",
    "Action": "ec2:CreateSnapshots",
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
     "Null": {
      "aws:TagKeys": "false"
     },
     "ForAllValues:StringEquals": {
      "aws:TagKeys": "InspectorScan"
     }
    }
   },
   {
    "Sid": "CreateOnlyInspectorScanTagOnlyUsingCreateSnapshots",
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
     "StringLike": {
      "ec2:CreateAction": "CreateSnapshots"
     },
     "Null": {
      "aws:TagKeys": "false"
     },
     "ForAllValues:StringEquals": {
      "aws:TagKeys": "InspectorScan"
     }
    }
   },
   {
    "Sid": "DeleteOnlySnapshotsTaggedForScanning",
    "Effect": "Allow",
    "Action": "ec2:DeleteSnapshot",
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
     "StringLike": {
```

```
      "ec2:ResourceTag/InspectorScan": "*"
     }
    }
   },
   {
    "Sid": "DenyKmsDecryptForExcludedKeys",
    "Effect": "Deny",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/InspectorEc2Exclusion": "true"
     }
    }
   },
   {
    "Sid": "DecryptSnapshotBlocksVolContext",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     },
     "StringLike": {
      "kms:ViaService": "ec2.*.amazonaws.com",
      "kms:EncryptionContext:aws:ebs:id": "vol-*"
     }
    }
   },
   {
    "Sid": "DecryptSnapshotBlocksSnapContext",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     },
     "StringLike": {
      "kms:ViaService": "ec2.*.amazonaws.com",
      "kms:EncryptionContext:aws:ebs:id": "snap-*"
     }
    }
```

```
  },
  {
   "Sid": "DescribeKeysForEbsOperations",
   "Effect": "Allow",
   "Action": "kms:DescribeKey",
   "Resource": "arn:aws:kms:*:*:key/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    },
    "StringLike": {
     "kms:ViaService": "ec2.*.amazonaws.com"
    }
   }
  },
  {
   "Sid": "ListKeyResourceTags",
   "Effect": "Allow",
   "Action": "kms:ListResourceTags",
   "Resource": "arn:aws:kms:*:*:key/*"
  }
 ]
}
```

## Criar um perfil vinculado ao serviço para verificação sem agente

Não é necessário criar manualmente uma função vinculada a serviço. Quando você ativa o Amazon Inspector na AWS Management Console, na ou na AWS API AWS CLI, o Amazon Inspector cria a função vinculada ao serviço para você.

## Editar um perfil vinculado ao serviço para verificação sem agente

O Amazon Inspector não permite que você edite a função vinculada ao serviço do `AWSServiceRoleForAmazonInspector2Agentless`. Após a criação da função vinculada a serviços, você não poderá alterar o nome da função, pois várias entidades podem fazer referência à função. No entanto, será possível editar a descrição da função usando o IAM. Para ter mais informações, consulte Editar um perfil vinculado ao serviço no Guia do usuário do IAM.

### Excluir um perfil vinculado ao serviço para verificação sem agente

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**
>
> Para excluir o perfil `AWSServiceRoleForAmazonInspector2Agentless`, você deve definir o modo de verificação baseado em agente em todas as regiões onde a verificação sem agente está disponível. Para obter mais informações, consulte [link do modo de digitalização de configuração a ser definido].

Como excluir manualmente a função vinculada a serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSServiceRoleForAmazonInspector2Agentless vinculada ao serviço. Para obter mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

## Solução de problemas de identidade e acesso do Amazon Inspector

Use as informações a seguir para ajudar a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o Amazon Inspector e o IAM.

Tópicos

- Não tenho autorização para executar uma ação no Amazon Inspector
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas de fora da minha acessem meus Conta da AWS recursos do Amazon Inspector

### Não tenho autorização para executar uma ação no Amazon Inspector

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `inspector2:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 inspector2: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 `inspector2:GetWidget`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

## Não estou autorizado a realizar iam: PassRole

Caso receba uma mensagem de erro informando que você não tem autorização para executar a ação, `iam:PassRole` as políticas deverão ser atualizadas para permitir a transmissão de um perfil para o Amazon Inspector.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O erro exemplificado a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para executar uma ação no Amazon Inspector. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

## Quero permitir que pessoas de fora da minha acessem meus Conta da AWS recursos do Amazon Inspector

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.

Para saber mais, consulte:

- Para saber se o Amazon Inspector é compatível com esses recursos, consulte Como o Amazon Inspector funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- 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.

# Monitorar o Amazon Inspector

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do Amazon Inspector e de suas outras AWS soluções. AWS fornece ferramentas de monitoramento para monitorar o Amazon Inspector, relatar quando algo está errado e tomar ações automáticas quando apropriado:

- EventBridgeA Amazon é um serviço de ônibus de eventos sem servidor que facilita a conexão de seus aplicativos com dados de várias fontes. EventBridge fornece um fluxo de dados em tempo real de seus próprios aplicativos, aplicativos S oftware-as-a -Service (SaaS) AWS e serviços e encaminha esses dados para destinos como o Lambda. Isso permite monitorar eventos que ocorrem em serviços e crie arquiteturas orientadas a eventos. Para obter mais informações, consulte o Guia EventBridge do usuário da Amazon.
- AWS CloudTrail captura chamadas de API e eventos relacionados realizados pela conta da Conta da AWS ou em nome dela. CloudTrail em seguida, entrega os arquivos de log para um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o

endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para mais informações, consulte o Guia do usuário do AWS CloudTrail.

## Log de chamadas de API do Amazon Inspector com o AWS CloudTrail

O Amazon Inspector está integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário ou função do IAM, ou um AWS service (Serviço da AWS), no Amazon Inspector. CloudTrail captura todas as chamadas de API para o Amazon Inspector como eventos. As chamadas capturadas incluem as chamadas do console do Amazon Inspector e as chamadas de código para as operações da API do Amazon Inspector. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Amazon Inspector. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar:

- A solicitação feita ao Amazon Inspector.
- O endereço IP do qual a solicitação foi feita.
- Quem fez a solicitação.
- Quando a solicitação foi feita.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

### Informações do Amazon Inspector em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no Amazon Inspector, essa atividade é registrada em um CloudTrail evento junto com outros AWS service (Serviço da AWS) eventos no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo de eventos em seu Conta da AWS, incluindo eventos para o Amazon Inspector, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra 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

Serviços da AWS para analisar e agir com base nos dados do evento coletados nos CloudTrail registros. Para obter mais informações, consulte os tópicos a seguir.

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurar notificações do Amazon SNS para o CloudTrail
- Recebendo arquivos de CloudTrail log de várias contas
- Recebendo arquivos de CloudTrail log de várias regiões

Todas as ações do Amazon Inspector são registradas por. CloudTrail Todas as ações que o Amazon Inspector pode realizar estão documentadas na Referência da API do Amazon Inspector. Por exemplo, chamadas para as `UpdateOrganizationConfiguration` ações `CreateFindingsReportListCoverage`, e geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário 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 AWS service (Serviço da AWS).

Para obter mais informações, consulte o elemento CloudTrail userIdentity.

## Noções básicas sobre entradas de arquivos de log do Amazon Inspector

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma solicitação única de qualquer fonte. Os eventos incluem informações sobre a ação solicitada, a data e hora da ação, os parâmetros de 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.

## Amazon Inspector Digitalize informações em CloudTrail

O Amazon Inspector Scan está integrado com o. CloudTrail Todas as operações da API Amazon Inspector Scan são registradas como eventos de gerenciamento. Para obter uma lista das operações

da API do Amazon Inspector Scan nas quais o Amazon Inspector se CloudTrail registra, consulte Amazon Inspector Scan na Referência da API do Amazon Inspector.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `ScanSbom` ação:


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA123456789EXAMPLE:akua_mansa",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/akua_mansa",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA123456789EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-10-17T15:22:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-10-17T16:02:34Z",
    "eventSource": "gamma-inspector-scan.amazonaws.com",
    "eventName": "ScanSbom",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.0",
    "userAgent": "aws-sdk-java/2.20.162 Mac_OS_X/13.5.2 OpenJDK_64-
Bit_Server_VM/17.0.8+7-LTS Java/17.0.8 vendor/Amazon.com_Inc. io/sync http/
UrlConnection cfg/retry-mode/legacy",
    "requestParameters": {
        "sbom": {
            "specVersion": "1.5",
            "metadata": {
                "component": {
                    "name": "debian",
                    "type": "operating-system",
```

```
                    "version": "9"
                }
            },
            "components": [
                {
                    "name": "packageOne",
                    "purl": "pkg:deb/debian/packageOne@1.0.0?arch=x86_64&distro=9",
                    "type": "application"
                }
            ],
            "bomFormat": "CycloneDX"
        }
    },
    "responseElements": null,
    "requestID": "f041a27f-f33e-4f70-b09b-5fbc5927282a",
    "eventID": "abc8d1e4-d214-4f07-bc56-8a31be6e36fe",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


# Validação de conformidade do Amazon Inspector

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

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

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

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.

- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

> **Note**
>
> Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte Referência dos Serviços Qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços com suporte e controles aceitos, consulte a Referência de controles do Security Hub.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

## Resiliência no Amazon Inspector

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente

disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

## Segurança da infraestrutura no Amazon Inspector

Como um serviço gerenciado, o Amazon Inspector é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o Amazon Inspector pela rede. Os clientes devem ser compatíveis com:

- 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, suporta esses modos.

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

## Resposta a incidentes no Amazon Inspector

A segurança é a maior prioridade na AWS. Como parte do modelo de responsabilidade compartilhada AWS na nuvem, AWS gerencia uma arquitetura de data center, rede e software que atende aos requisitos das organizações mais sensíveis à segurança. AWS é responsável por qualquer resposta a incidentes com relação ao AWS Config serviço em si. Além disso, como AWS cliente, você compartilha a responsabilidade de manter a segurança na nuvem. Isso significa que você controla a segurança que escolhe implementar a partir das AWS ferramentas e recursos aos quais tem acesso e é responsável pela resposta a incidentes do seu lado do modelo de responsabilidade compartilhada.

Ao estabelecer um nível básico de segurança que atenda aos objetivos de seus aplicativos executados na nuvem, você pode detectar desvios aos quais pode reagir. Como a resposta a

incidentes de segurança pode ser um tópico complexo, recomendamos que você analise os seguintes recursos para entender melhor o impacto que a resposta a incidentes (IR) e suas escolhas têm em suas metas corporativas: Guia de resposta a incidentes de AWS segurança, whitepaper de melhores práticas de AWS segurança e white paper sobre a perspectiva de segurança da estrutura de adoção de AWS nuvem (CAF).

# Integrações no Amazon Inspector

O Amazon Inspector se integra com outros serviços. AWS Esses serviços podem ingerir dados do Amazon Inspector para permitir visualizar suas descobertas de novas maneiras. Veja as opções de integração a seguir para saber mais sobre como cada serviço funciona com o Amazon Inspector.

## Integração do Amazon Inspector com o Amazon ECR

O Amazon Elastic Container Registry (Amazon ECR) é um registro de contêiner do Docker totalmente gerenciado que facilita o armazenamento, o gerenciamento, o compartilhamento e a implantação de imagens de contêiner. Os registros privados do Amazon ECR hospedam as imagens de contêiner em uma arquitetura altamente disponível e escalável. Use o Amazon Inspector para verificar as imagens de contêineres que residem em seus repositórios do Amazon ECR em busca de pacotes vulneráveis do sistema operacional e pacotes de linguagem de programação.

Para obter mais informações sobre como usar o Amazon ECR com o Amazon Inspector, consulte Integração do Amazon Inspector ao Amazon Elastic Container Registry (Amazon ECR).

## Integração do Amazon Inspector com AWS Security Hub

AWS Security Hubcoleta dados de segurança de suas AWS contas, serviços e outros produtos compatíveis para avaliar o estado de segurança do seu ambiente de acordo com os padrões e as melhores práticas do setor. Além de avaliar sua postura de segurança, o Security Hub cria um local central para descobertas em todos os seus AWS serviços integrados e produtos da AWS Partner Network. A ativação do Security Hub com o Amazon Inspector permite automaticamente que o Security Hub consuma dados de descobertas do Amazon Inspector.

Para ter mais informações sobre usar o Security Hub com o Amazon Inspector, consulte Integração do Amazon Inspector com AWS Security Hub.

## Integração do Amazon Inspector ao Amazon Elastic Container Registry (Amazon ECR)

O Amazon ECR é um registro de contêineres totalmente gerenciado que oferece suporte a imagens e artefatos Docker e OCI em AWS. Se estiver usando o Amazon ECR, você poderá ativar o Escaneamento avançado para seu registro para permitir que o Amazon Inspector detecte

automaticamente as imagens do seu contêiner e as verifique em busca de pacotes vulneráveis do sistema operacional e pacotes de linguagem de programação.

Essa integração permite visualizar as descobertas do Amazon Inspector para imagens de contêineres no console do Amazon ECR. Além disso, no console do Amazon ECR, você poderá gerenciar a frequência de verificação e refinar o escopo das verificações criando filtros de inclusão.

### Ativar a integração

Ative a integração ao ativar o escaneamento do Amazon Inspector por meio do console ou da API do Amazon Inspector, ou configurando seu repositório para usar o Escaneamento avançado com o Amazon Inspector por meio do console ou da API do Amazon ECR.

Para obter mais informações sobre a ativação da integração por meio do Amazon Inspector, consulte. Verificação automatizada de recursos do Amazon Inspector

Para obter informações sobre como ativar e configurar o Escaneamento avançado no Amazon ECR, consulte Escaneamento avançado no guia do usuário do Amazon ECR.

### Usar a integração com um ambiente de várias contas

Se for membro de um ambiente com várias contas, poderá ativar o escaneamento avançado por meio do Amazon ECR. No entanto, uma vez ativado, ele só pode ser desativado pelo administrador delegado do Amazon Inspector. Se estiver desativado, ele será revertido ao escaneamento básico. Para ter mais informações, consulte Desativar o Amazon Inspector.

## Integração do Amazon Inspector com AWS Security Hub

O Security Hub fornece uma visão abrangente do seu estado de segurança AWS e ajuda você a verificar seu ambiente de acordo com os padrões e as melhores práticas do setor de segurança. O Security Hub coleta dados de segurança de várias AWS contas, serviços e produtos adicionais compatíveis. Use as informações fornecidas para analisar suas tendências de segurança e a identificar os problemas de segurança de maior prioridade.

A integração do Amazon Inspector com o Security Hub permite enviar descobertas do Amazon Inspector ao Security Hub. O Security Hub pode então incluir tais descobertas na análise feita sobre a seu procedimento de segurança.

Em AWS Security Hub, os problemas de segurança são rastreados como descobertas. Algumas descobertas resultam de problemas detectados por outros AWS serviços ou por produtos de

terceiros. 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. É possível exibir e filtrar listas de descobertas e exibir detalhes das descobertas. Para obter mais informações sobre descobertas no Security Hub, consulte Como exibir descobertas no Guia do usuário do AWS Security Hub . Você também pode rastrear o status de uma investigação em uma descoberta. Consulte Tomar medidas sobre descobertas no Guia 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 .

O Security Hub arquivará as descobertas do Amazon Inspector assim que essas descobertas forem abordadas e encerradas no Amazon Inspector.

## Visualizar as descobertas do Amazon Inspector em AWS Security Hub

As descobertas do Amazon Inspector Classic e do novo Amazon Inspector estão disponíveis no mesmo painel no Security Hub. No entanto, você poderá filtrar as descobertas do novo Amazon Inspector adicionando um `"aws/inspector/ProductVersion": "2"` à barra de filtro. Adicionar esse filtro exclui as descobertas do Amazon Inspector Classic do painel do Security Hub.

Exemplo de descoberta do Amazon Inspector


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:inspector2:us-east-1:123456789012:finding/FINDING_ID",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
  "ProductName": "Inspector",
  "CompanyName": "Amazon",
  "Region": "us-east-1",
  "GeneratorId": "AWSInspector",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
  ],
  "FirstObservedAt": "2023-01-31T20:25:38Z",
  "LastObservedAt": "2023-05-04T18:18:43Z",
  "CreatedAt": "2023-01-31T20:25:38Z",
  "UpdatedAt": "2023-05-04T18:18:43Z",
```

```
  "Severity": {
    "Label": "HIGH",
    "Normalized": 70
  },
  "Title": "CVE-2022-34918 - kernel",
  "Description": "An issue was discovered in the Linux kernel through 5.18.9. A type
 confusion bug in nft_set_elem_init (leading to a buffer overflow) could be used by a
 local attacker to escalate privileges, a different vulnerability than CVE-2022-32250.
 (The attacker can obtain root access, but must start with an unprivileged user
 namespace to obtain CAP_NET_ADMIN access.) This can be fixed in nft_setelem_parse_data
 in net/netfilter/nf_tables_api.c.",
  "Remediation": {
    "Recommendation": {
      "Text": "Remediation is available. Please refer to the Fixed version in the
 vulnerability details section above. For detailed remediation guidance for each of the
 affected packages, refer to the vulnerabilities section of the detailed finding JSON."
    }
  },
  "ProductFields": {
    "aws/inspector/FindingStatus": "ACTIVE",
    "aws/inspector/inspectorScore": "7.8",
    "aws/inspector/resources/1/resourceDetails/awsEc2InstanceDetails/platform":
 "AMAZON_LINUX_2",
    "aws/inspector/ProductVersion": "2",
    "aws/inspector/instanceId": "i-0f1ed287081bdf0fb",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/inspector/
arn:aws:inspector2:us-east-1:123456789012:finding/FINDING_ID",
    "aws/securityhub/ProductName": "Inspector",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:123456789012:i-0f1ed287081bdf0fb",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Patch Group": "SSM",
        "Name": "High-SEv-Test"
      },
      "Details": {
        "AwsEc2Instance": {
          "Type": "t2.micro",
          "ImageId": "ami-0cff7528ff583bf9a",
```

```
          "IpV4Addresses": [
            "52.87.229.97",
            "172.31.57.162"
          ],
          "KeyName": "ACloudGuru",
          "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/
AmazonSSMRoleForInstancesQuickSetup",
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-9c934cb1",
          "LaunchedAt": "2022-07-26T21:49:46Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "Vulnerabilities": [
    {
      "Id": "CVE-2022-34918",
      "VulnerablePackages": [
        {
          "Name": "kernel",
          "Version": "5.10.118",
          "Epoch": "0",
          "Release": "111.515.amzn2",
          "Architecture": "X86_64",
          "PackageManager": "OS",
          "FixedInVersion": "0:5.10.130-118.517.amzn2",
          "Remediation": "yum update kernel"
        }
      ],
      "Cvss": [
        {
          "Version": "2.0",
          "BaseScore": 7.2,
          "BaseVector": "AV:L/AC:L/Au:N/C:C/I:C/A:C",
          "Source": "NVD"
        },
        {
          "Version": "3.1",
          "BaseScore": 7.8,
```

```
          "BaseVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
          "Source": "NVD"
        },
        {
          "Version": "3.1",
          "BaseScore": 7.8,
          "BaseVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
          "Source": "NVD",
          "Adjustments": []
        }
      ],
      "Vendor": {
        "Name": "NVD",
        "Url": "https://nvd.nist.gov/vuln/detail/CVE-2022-34918",
        "VendorSeverity": "HIGH",
        "VendorCreatedAt": "2022-07-04T21:15:00Z",
        "VendorUpdatedAt": "2022-10-26T17:05:00Z"
      },
      "ReferenceUrls": [
        "https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?
id=7e6bc1f6cabcd30aba0b11219d8e01b952eacbb6",
        "https://lore.kernel.org/netfilter-devel/cd9428b6-7ffb-dd22-d949-
d86f4869f452@randorisec.fr/T/",
        "https://www.debian.org/security/2022/dsa-5191"
      ],
      "FixAvailable": "YES"
    }
  ],
  "FindingProviderFields": {
    "Severity": {
      "Label": "HIGH"
    },
    "Types": [
      "Software and Configuration Checks/Vulnerabilities/CVE"
    ]
  },
  "ProcessedAt": "2023-05-05T20:28:38.822Z"
}
```

## Ativar e configurar a integração

Para usar a integração do Amazon Inspector com AWS Security Hub, você deve ativar o Security Hub. Para obter informações sobre como ativar o Hub de segurança, consulte Configurar o Security Hub no Guia do usuário do AWS Security Hub .

Ao ativar o Amazon Inspector e o Security Hub, a integração é ativada automaticamente e o Amazon Inspector começa a enviar descobertas ao Security Hub. O Amazon Inspector envia todas as descobertas para o Security Hub usando o ASFF (Formato de descoberta de segurança da) da AWS.

## Interrompendo a publicação de descobertas para AWS Security Hub

Como parar de enviar descobertas

Para interromper o envio das descobertas ao Security Hub, você poderá usar o console ou a API do Security Hub.

Consulte Desativar e ativar o fluxo de descobertas de uma integração (console) ou Desativar o fluxo de descobertas de uma integração (API do Security Hub, AWS CLI) no Guia do usuário do AWS Security Hub .

# Sistemas operacionais e linguagens de programação com suporte pelo Amazon Inspector

O Amazon Inspector pode escanear aplicativos de software instalados em instâncias do Amazon Elastic Compute Cloud (Amazon EC2), imagens de contêineres armazenadas em repositórios e funções do Amazon Elastic Container Registry (Amazon ECR). AWS Lambda Para imagens de contêineres ECR, o Amazon Inspector pode verificar as vulnerabilidades do sistema operacional e do pacote de linguagem de programação. Para funções Lambda, o Amazon Inspector pode escanear vulnerabilidades de código. Quando o Amazon Inspector verifica os recursos, ele usa seu próprio mecanismo de verificação criado especificamente e fornece mais de 50 feeds de dados para gerar descobertas sobre as CVEs (vulnerabilidades e exposições comuns). As fontes incluem recomendações de segurança de fornecedores, NVD, MITRE, feeds de código aberto, pesquisas internas e feeds de dados licenciados.

Para que o Amazon Inspector verifique um recurso, o recurso deve estar executando um sistema operacional compatível ou usar uma linguagem de programação compatível. Os tópicos desta seção listam os sistemas operacionais, os tempos de execução e as linguagens de programação que o Amazon Inspector atualmente suporta para diferentes recursos e tipos de escaneamento. Eles também listam sistemas operacionais que o Amazon Inspector suportava anteriormente, mas que foram descontinuados pelos fornecedores. O Amazon Inspector só pode fornecer suporte limitado para um sistema operacional depois que um fornecedor interrompe o suporte para o sistema operacional.

Tópicos

# Sistemas operacionais com suporte: ao escaneamento do Amazon EC2

A tabela a seguir lista os sistemas operacionais que o Amazon Inspector atualmente suporta para escaneamentos de instâncias do Amazon EC2. Ele também lista a origem dos alertas de segurança do fornecedor para cada um e se esse sistema operacional pode ser verificado usando o método de verificação baseado em agente ou sem agente. Para obter mais informações sobre métodos de verificação, consulte Verificação baseada em agente e Verificação sem agente.

> **Note**
>
> As detecções do sistema operacional Linux são suportadas somente pelo repositório padrão do gerenciador de pacotes e não incluem aplicativos de terceiros, repositórios de suporte estendido (por exemplo, BYOS RHEL, PAYG RHEL e RHEL for SAP) e repositórios opcionais, como o Red Hat Application Streams.

| Sistema operacional | Version (Versão) | Recomendações de segurança do fornecedor | Suporte para verificação sem agente | Suporte de verificação baseada em agente |
|---|---|---|---|---|
| AlmaLinux | 8 | ALSA | Sim | Sim |
| AlmaLinux | 9 | ALSA | Sim | Sim |
| Amazon Linux (AL2) | AL2 | ALAS | Sim | Sim |
| Amazon Linux 2023 (AL2023) | AL2023 | ALAS | Sim | Sim |
| Bottlerocket | 1.7.0 e versões posteriores | GHSA, CVE | Não | Sim |
| CentOS Linux (CentOS) | 7 | CESA | Sim | Sim |

| Sistema operacional | Version (Versão) | Recomendações de segurança do fornecedor | Suporte para verificação sem agente | Suporte de verificação baseada em agente |
|---|---|---|---|---|
| Servidor Debian (Buster) | 10 | DSA | Sim | Sim |
| Servidor Debian (Bullseye) | 11 | DSA | Sim | Sim |
| Servidor Debian (Bookworm) | 12 | DSA | Sim | Sim |
| Fedora | 38 | CVE | Sim | Sim |
| Fedora | 39 | CVE | Sim | Sim |
| OpenSUSE | 15,5 | CVE | Sim | Sim |
| Oracle Linux (Oracle) | 7 | ELSA | Sim | Sim |
| Oracle Linux (Oracle) | 8 | ELSA | Sim | Sim |
| Oracle Linux (Oracle) | 9 | ELSA | Sim | Sim |
| Red Hat Enterprise Linux (RHEL) | 7 | RHSA | Sim | Sim |
| Red Hat Enterprise Linux (RHEL) | 8 | RHSA | Sim | Sim |

| Sistema operacional | Version (Versão) | Recomendações de segurança do fornecedor | Suporte para verificação sem agente | Suporte de verificação baseada em agente |
|---|---|---|---|---|
| Red Hat Enterprise Linux (RHEL) | 9 | RHSA | Sim | Sim |
| Rocky Linux | 8 | RLSA | Sim | Sim |
| Rocky Linux | 9 | RLSA | Sim | Sim |
| SLES (SUSE Linux Enterprise Server) | 12.4 | SUSE CVE | Sim | Sim |
| SLES (SUSE Linux Enterprise Server) | 12,5 | SUSE CVE | Sim | Sim |
| SLES (SUSE Linux Enterprise Server) | 15.3 | SUSE CVE | Sim | Sim |
| SLES (SUSE Linux Enterprise Server) | 15.4 | SUSE CVE | Sim | Sim |
| SLES (SUSE Linux Enterprise Server) | 15,5 | SUSE CVE | Sim | Sim |
| Ubuntu (Confiável) | 14.04 (ESM) | USN, Ubuntu Pro | Sim | Sim |
| Ubuntu (Xenial) | 16.04 (ESM) | USN, Ubuntu Pro | Sim | Sim |

| Sistema operacional | Version (Versão) | Recomendações de segurança do fornecedor | Suporte para verificação sem agente | Suporte de verificação baseada em agente |
|---|---|---|---|---|
| Ubuntu (Biônico) | 18.04 (ESM) | USN, Ubuntu Pro | Sim | Sim |
| Ubuntu (Focal) | 20.04 (LTS) | USN | Sim | Sim |
| Ubuntu (Jammy) | 22.04 (LTS) | USN | Sim | Sim |
| Ubuntu (Mantic Minotaur) | 23.10 | USN | Sim | Sim |
| Windows Server | 2016 | MSKB | Não | Sim |
| Windows Server | 2019 | MSKB | Não | Sim |
| Windows Server | 2022 | MSKB | Não | Sim |
| macOS (Mojave) | 10.14 | APPLE-SA | Não | Sim |
| macOS (Catalina) | 10.15 | APPLE-SA | Não | Sim |
| macOS (Big Sur) | 11 | APPLE-SA | Não | Sim |
| macOS (Monterey) | 12 | APPLE-SA | Não | Sim |
| macOS (Ventura) | 13 | APPLE-SA | Não | Sim |

# Linguagens de programação suportadas: inspeção profunda do Amazon EC2

Atualmente, o Amazon Inspector suporta as seguintes linguagens de programação ao escanear instâncias Linux do Amazon EC2 em busca de vulnerabilidades em pacotes de software de terceiros:

- Java
- JavaScript
- Python

O Amazon Inspector usa o Systems Manager Distributor para implantar o plug-in usado para inspeção profunda em sua instância do Amazon EC2. O distribuidor do Gerenciador de Sistemas dá suporte aos sistemas operacionais listados como Plataformas e arquiteturas de pacotes com suporte no guia do Gerenciador de Sistemas. O sistema operacional da sua instância do Amazon EC2 deve ser compatível com o Systems Manager Distributor e o Amazon Inspector para que o Amazon Inspector execute verificações de inspeção detalhadas.

> **Note**
>
> A inspeção profunda não tem suporte pelos sistemas operacionais Bottlerocket.

## Sistemas operacionais suportados: digitalização CIS

A tabela a seguir lista os sistemas operacionais que o Amazon Inspector atualmente suporta para escaneamentos do CIS. A tabela também inclui a versão de benchmark do CIS usada para realizar varreduras desse sistema operacional.

| Sistema operacional | Version (Versão) | Versão de referência do CIS |
|---|---|---|
| Amazon Linux 2 | AL2 | 2.0.0 |
| Amazon Linux 2023 | AL2023 | 1.0.0 |
| Windows Server | 2019 | 2.0.0 |
| Windows Server | 2022 | 2.0.0 |

# Sistemas operacionais suportados: digitalização do Amazon ECR com o Amazon Inspector

Atualmente, o Amazon Inspector suporta a digitalização dos seguintes sistemas operacionais ao digitalizar imagens de contêineres nos repositórios do Amazon ECR:. A tabela também lista a origem das recomendações de segurança do fornecedor para cada sistema operacional.

| Sistema operacional | Version (Versão) | Recomendações de segurança do fornecedor |
|---|---|---|
| Alpine Linux (Alpine) | 3.16 | Alpine SecDB |
| Alpine Linux (Alpine) | 3.17 | Alpine SecDB |
| Alpine Linux (Alpine) | 3.18 | Alpine SecDB |
| Alpine Linux (Alpine) | 3.19 | Alpine SecDB |
| AlmaLinux | 8 | ALSA |
| AlmaLinux | 9 | ALSA |
| Amazon Linux (AL2) | AL2 | ALAS |
| Amazon Linux 2023 (AL2023) | AL2023 | ALAS |
| CentOS Linux (CentOS) | 7 | CESA |
| Debian Server (Buster) | 10 | DSA |
| Debian Server (Bullseye) | 11 | DSA |
| Debian Server (Bookworm) | 12 | DSA |
| Fedora | 38 | CVE |
| Fedora | 39 | CVE |
| OpenSUSE | 15.5 | CVE |

| Sistema operacional | Version (Versão) | Recomendações de segurança do fornecedor |
|---|---|---|
| Oracle Linux (Oracle) | 7 | ELSA |
| Oracle Linux (Oracle) | 8 | ELSA |
| Oracle Linux (Oracle) | 9 | ELSA |
| Photon OS | 3 | PHSA |
| Photon OS | 4 | PHSA |
| Photon OS | 5 | PHSA |
| Red Hat Enterprise Linux (RHEL) | 7 | RHSA |
| Red Hat Enterprise Linux (RHEL) | 8 | RHSA |
| Red Hat Enterprise Linux (RHEL) | 9 | RHSA |
| Rocky Linux | 8 | RLSA |
| Rocky Linux | 9 | RLSA |
| SUSE Linux Enterprise Server (SLES) | 12.4 | SUSE CVE |
| SUSE Linux Enterprise Server (SLES) | 12.5 | SUSE CVE |
| SUSE Linux Enterprise Server (SLES) | 15.3 | SUSE CVE |
| SUSE Linux Enterprise Server (SLES) | 15.4 | SUSE CVE |

| Sistema operacional | Version (Versão) | Recomendações de segurança do fornecedor |
|---|---|---|
| SUSE Linux Enterprise Server (SLES) | 15.5 | SUSE CVE |
| Ubuntu (Trusty) | 14.04 (ESM) | USN, Ubuntu Pro |
| Ubuntu (Xenial) | 16.04 (ESM) | USN, Ubuntu Pro |
| Ubuntu (Bionic) | 18.04 (ESM) | USN, Ubuntu Pro |
| Ubuntu (Focal) | 20.04 (LTS) | USN |
| Ubuntu (Jammy) | 22.04 (LTS) | USN |
| Ubuntu (Mantic Minotaur) | 23.10 | USN |

# Linguagens de programação com suporte: ao escaneamento do Amazon ECR

Atualmente, o Amazon Inspector suporta as seguintes linguagens de programação ao digitalizar imagens de contêineres nos repositórios do Amazon ECR:

- C#
- Go
- Java
- JavaScript
- PHP
- Python
- Ruby
- Rust

# Runtime com suporte: ao escaneamento padrão do Lambda do Amazon Inspector

O escaneamento padrão do Amazon Inspector Lambda atualmente suporta as seguintes linguagens de programação ao escanear funções do Lambda em busca de vulnerabilidades em pacotes de software de terceiros:

- Java
  - java8
  - java8.al2
  - java11
  - java17
- Node.js
  - nodejs12.x
  - nodejs14.x
  - nodejs16.x
  - nodejs18.x
  - nodejs20.x
- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
- Go
  - go1.x
- Ruby
  - ruby2.7
  - ruby3.2
- .NET
  - .NET 6

# Runtime com suporte: ao escaneamento de código do Lambda do Amazon Inspector

O escaneamento de código do Amazon Inspector Lambda atualmente suporta as seguintes linguagens de programação ao escanear funções do Lambda em busca de vulnerabilidades no código:

- Java
  - java8
  - java8.al2
  - java11
  - java17
- Node.js
  - nodejs12.x
  - nodejs14.x
  - nodejs16.x
  - nodejs18.x
  - nodejs20.x
- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
- Ruby
  - ruby2.7
  - ruby3.2

# Sistemas operacionais descontinuados

O suporte padrão do fornecedor para os sistemas operacionais listados nas tabelas a seguir foi descontinuado pelo fornecedor. Nas tabelas, a coluna Descontinuado indica quando o fornecedor interrompeu o suporte padrão para um sistema operacional.

Anteriormente, o Amazon Inspector fornecia suporte completo para esses sistemas operacionais e continuará a escanear as instâncias do Amazon EC2 e as imagens de contêineres do Amazon ECR que as estão executando. No entanto, de acordo com a política do fornecedor, os sistemas operacionais não são mais atualizados com patches e, em muitos casos, novos avisos de segurança não são mais lançados para eles. Além disso, alguns fornecedores removem os alertas e detecções de segurança existentes de seus feeds quando um sistema operacional afetado chega ao fim do suporte padrão. Consequentemente, o Amazon Inspector pode parar de gerar descobertas para CVEs conhecidas. Qualquer descoberta que o Amazon Inspector gerar para um sistema operacional descontinuado deve ser usada apenas para fins informativos.

Como melhor prática de segurança e para a cobertura contínua do Amazon Inspector, é recomendável mudar para uma versão atual e com suporte de um sistema operacional.

Sistemas operacionais descontinuados: escaneamento do Amazon EC2

| Sistema operacional | Version (Versão) | Descontinuado |
|---|---|---|
| Amazon Linux (AL1) | 2012 | 31 de dezembro de 2021 |
| CentOS Linux (CentOS) | 8 | 31 de dezembro de 2021 |
| Servidor Debian (Stretch) | 9 | 30 de junho de 2022 |
| Fedora | 35 | 13 de dezembro de 2022 |
| Fedora | 36 | 16 de maio de 2023 |
| Fedora | 37 | 5 de dezembro de 2023 |
| OpenSUSE | 15.3 | 1º de dezembro de 2022 |
| OpenSUSE | 15.4 | 7 de dezembro de 2023 |

| Sistema operacional | Version (Versão) | Descontinuado |
| --- | --- | --- |
| OpenSUSE Leap (SUSE Leap) | 15.2 | 1º de dezembro de 2021 |
| Oracle Linux (Oracle) | 6 | 1º de março de 2021 |
| SLES (SUSE Linux Enterprise Server) | 12 | 1 de julho de 2019 |
| SLES (SUSE Linux Enterprise Server) | 12.1 | 31 de maio de 2020 |
| SLES (SUSE Linux Enterprise Server) | 12.2 | 31 de março de 2021 |
| SLES (SUSE Linux Enterprise Server) | 12.3 | 30 de junho de 2022 |
| SLES (SUSE Linux Enterprise Server) | 15 | 31 de dezembro de 2019 |
| SLES (SUSE Linux Enterprise Server) | 15.1 | 31 de janeiro de 2021 |
| SLES (SUSE Linux Enterprise Server) | 15.2 | 31 de dezembro de 2021 |
| Ubuntu (Groovy) | 20.10 | 22 de julho de 2021 |
| Ubuntu (hirsuto) | 21,04 | 20 de janeiro de 2022 |
| Ubuntu (travesso) | 21.10 | 31 de julho de 2022 |
| Ubuntu (Kinetic) | 22.10 | July 20, 2023 |
| Ubuntu (Lunar Lobster) | 23.04 | January 25, 2024 |
| Windows Server | 2012 | 10 de outubro de 2023 |
| Windows Server | 2012 R2 | 10 de outubro de 2023 |

## Sistemas operacionais descontinuados: escaneamento do Amazon ECR

| Sistema operacional | Version (Versão) | Descontinuado |
|---|---|---|
| Alpine Linux (Alpino) | 3.12 | 1º de maio de 2022 |
| Alpine Linux (Alpino) | 3.13 | 1º de novembro de 2022 |
| Alpine Linux (Alpine) | 3.14 | May 1, 2023 |
| Alpine Linux (Alpine) | 3.15 | November 1, 2023 |
| Amazon Linux (AL1) | 2012 | 31 de dezembro de 2021 |
| CentOS Linux (CentOS) | 8 | 31 de dezembro de 2021 |
| Servidor Debian (Stretch) | 9 | 30 de junho de 2022 |
| Fedora | 35 | 13 de dezembro de 2022 |
| Fedora | 36 | 16 de maio de 2023 |
| OpenSUSE | 15.3 | 1º de dezembro de 2022 |
| OpenSUSE | 15.4 | December 7, 2023 |
| OpenSUSE Leap (SUSE Leap) | 15.2 | 1º de dezembro de 2021 |
| Oracle Linux (Oracle) | 6 | 1º de março de 2021 |
| SLES (SUSE Linux Enterprise Server) | 12 | 1 de julho de 2019 |
| SLES (SUSE Linux Enterprise Server) | 12.1 | 31 de maio de 2020 |
| SLES (SUSE Linux Enterprise Server) | 12.2 | 31 de março de 2021 |

| Sistema operacional | Version (Versão) | Descontinuado |
| --- | --- | --- |
| SLES (SUSE Linux Enterprise Server) | 12.3 | 30 de junho de 2022 |
| SLES (SUSE Linux Enterprise Server) | 15 | 31 de dezembro de 2019 |
| SLES (SUSE Linux Enterprise Server) | 15.1 | 31 de janeiro de 2021 |
| SLES (SUSE Linux Enterprise Server) | 15.2 | 31 de dezembro de 2021 |
| Ubuntu (Groovy) | 20.10 | 22 de julho de 2021 |
| Ubuntu (hirsuto) | 21,04 | 20 de janeiro de 2022 |
| Ubuntu (travesso) | 21.10 | 31 de julho de 2022 |
| Ubuntu (Kinetic) | 22.10 | July 20, 2023 |
| Ubuntu (Lunar Lobster) | 23.04 | January 25, 2024 |

# Desativar o Amazon Inspector

Você pode desativar o Amazon Inspector em Região da AWS qualquer um usando o console ou a API do Amazon Inspector. Siga as instruções no final deste tópico para desativar o Amazon Inspector. Se você desativar todas as digitalizações do Amazon Inspector para uma, o Conta da AWS Amazon Inspector será desativado automaticamente para essa conta. Para obter informações sobre a desativação de tipos de verificação para diferentes recursos, consulte Verificação automatizada de recursos do Amazon Inspector.

Depois que o Amazon Inspector é desativado para uma conta, todos os tipos de verificação são desativados para essa conta nessa região. Além disso, todas as configurações de verificação, regras de supressão, filtros e descobertas do Amazon Inspector para a conta nessa região são excluídos.

Você não será cobrado pelo uso do Amazon Inspector enquanto ele estiver desativado para sua conta nessa região. Depois de desativar o Amazon Inspector, você poderá optar por reativá-lo mais tarde.

> **Note**
>
> Antes de desativar o Amazon Inspector, é recomendável exportar suas descobertas. Para ter mais informações, consulte Exportação de relatórios de descobertas do Amazon Inspector.

Ao desativar a verificação do Amazon EC2 do Amazon Inspector, as seguintes associações de SSM usadas pelo Amazon Inspector são excluídas:

- `InspectorDistributor-do-not-delete`
- `InspectorInventoryCollection-do-not-delete`
- `InvokeInspectorSsmPlugin-do-not-delete`. Além disso, o plug-in Amazon Inspector SSM instalado por meio dessa associação é removido de todos os seus hosts. Windows Para ter mais informações, consulte Verificação das instâncias do Windows..

Pré-requisitos

Dependendo do seu tipo de conta, talvez seja necessário tomar medidas adicionais antes de desativar o Amazon Inspector da seguinte forma:

- Caso tiver uma conta autônoma do Amazon Inspector, poderá desativá-la a qualquer momento.
- Se for uma conta membro em um ambiente de várias contas do Amazon Inspector, não poderá desativar seu próprio serviço. Entre em contato com o administrador delegado da sua organização para desativar seu serviço.
- Se você for um administrador delegado, você deve desassociar todas as suas contas de membros antes de poder desativar o Amazon Inspector. Para ter mais informações, consulte Desassociar contas-membro no Amazon Inspector.

> **Note**
>
> Desassociar uma conta não desativa o Amazon Inspector para essa conta, em vez disso, uma conta de membro desassociada se torna uma conta independente.

> **Note**
>
> Ao desativar o Amazon Inspector como administrador delegado, o recurso de ativação automática é desativado para sua organização.

# Desativar Amazon Inspector

Console

Para desativar o Amazon Inspector

1. Abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/v2/home.
2. Ao usar o Região da AWS seletor no canto superior direito da página, escolha a região na qual você deseja desativar o Amazon Inspector.
3. No painel de navegação, selecione Configurações gerais.
4. Selecione a opção Desativar o Inspector.
5. Quando solicitada a confirmação, digite desativar na caixa de texto e, em seguida, escolha Desativar o Inspector.
6. (Recomendado) Repita essas etapas em cada região da qual deseja desativar o Amazon Inspector.

### API

Execute a operação Desativar da API. Na solicitação, forneça os IDs da conta que você está desativando e `EC2, ECR, LAMBDA` para os `resourceTypes`, para desativar todas as verificações, o que desativará a conta.

# Cotas do Amazon Inspector

Sua AWS conta tem as seguintes cotas para o Amazon Inspector por região.

| Recurso | Padrão | Comentários |
| --- | --- | --- |
| Regras de supressão | 500 | O número máximo de regras de supressão salvas por AWS conta por região.<br><br>Não é possível solicitar um aumento da cota. |
| Descobertas da rede do Amazon EC2 | 10.000 | O número máximo de descobertas de rede do Amazon EC2 por conta. AWS<br><br>Não é possível solicitar um aumento da cota. |
| Contas-membro | 10000 | O número máximo de contas de membro associadas a uma conta de administrador delegado do Amazon Inspector. Esse limite é baseado em AWS Organizations, consulte Cotas para AWS Organizations. |

| Recurso | Padrão | Comentários |
| --- | --- | --- |
| Configurações de digitalização CIS | 500 | O número máximo de configurações de escaneamento CIS.<br><br>Não é possível solicitar um aumento da cota. |

Para obter uma lista de cotas associadas ao Amazon Inspector Classic, consulte as Service Quotas do Amazon Inspector no Referência geral da AWS.

Para obter uma lista de cotas associadas ao Organizações, consulte Service Quotas do Organizações no Referência geral da AWS.

# Regiões e endpoints

A verificação sem agente do Amazon Inspector para o Amazon EC2 está em versão prévia. O uso do recurso de verificação sem agente do Amazon EC2 está sujeito à Seção 2 dos Termos de serviço da AWS ("Betas e versões prévias").

Para ver Regiões da AWS onde o Amazon Inspector está disponível, consulte os endpoints do Amazon Inspector no. Referência geral da Amazon Web Services

## Endpoints para API Amazon Inspector Scan

A tabela a seguir mostra os endpoints regionais que podem ser usados ao chamar a API Amazon Inspector Scan. Ao usar a API, você deve fornecer o endpoint e a região correspondente para a AWS região na qual você está autenticado no momento.

A convenção de nomenclatura para endpoints do Amazon Inspector Scan é `inspector-scan.`*`region`*`.amazonaws.com`. Por exemplo, se você estiver autenticado em `us-west-2`, você usaria o endpoint `inspector-scan.us-west-2.amazonaws.com` para chamar a API `inspector-scan`.

| Nome da região | Região | Endpoint | Protocolo |
|---|---|---|---|
| Leste dos EUA (Ohio) | us-east-2 | inspector-scan.us-east-2.amazonaws.com<br><br>inspector-scan-fips.us-east-2.amazonaws.com | HTTPS |
| Leste dos EUA (Norte da Virgínia) | us-east-1 | inspector-scan.us-east-1.amazonaws.com | HTTPS |

| Nome da região | Região | Endpoint | Protocolo |
| --- | --- | --- | --- |
| | | inspector-scan-fips.us-east-1.amazonaws.com | |
| Oeste dos EUA (Norte da Califórnia) | us-west-1 | inspector-scan.us-west-1.amazonaws.com<br><br>inspector-scan-fips.us-west-1.amazonaws.com | HTTPS |
| Oeste dos EUA (Oregon) | us-west-2 | inspector-scan.us-west-2.amazonaws.com<br><br>inspector-scan-fips.us-west-2.amazonaws.com | HTTPS |
| África (Cidade do Cabo) | af-south-1 | inspector-scan.af-south-1.amazonaws.com | HTTPS |
| Ásia-Pacífico (Hong Kong) | ap-east-1 | inspector-scan.ap-east-1.amazonaws.com | HTTPS |
| Ásia-Pacífico (Jacarta) | ap-southeast-3 | inspector-scan.ap-southeast-3.amazonaws.com | HTTPS |
| Ásia-Pacífico (Mumbai) | ap-south-1 | inspector-scan.ap-south-1.amazonaws.com | HTTPS |

| Nome da região | Região | Endpoint | Protocolo |
| --- | --- | --- | --- |
| Asia Pacific (Osaka) | ap-northeast-3 | inspector-scan.ap-northeast-3.amazonaws.com | HTTPS |
| Ásia-Pacífico (Seul) | ap-northeast-2 | inspector-scan.ap-northeast-2.amazonaws.com | HTTPS |
| Ásia-Pacífico (Singapura) | ap-southeast-1 | inspector-scan.ap-southeast-1.amazonaws.com | HTTPS |
| Ásia-Pacífico (Sydney) | ap-southeast-2 | inspector-scan.ap-southeast-2.amazonaws.com | HTTPS |
| Ásia-Pacífico (Tóquio) | ap-northeast-1 | inspector-scan.ap-northeast-1.amazonaws.com | HTTPS |
| Canadá (Central) | ca-central-1 | inspector-scan.ca-central-1.amazonaws.com | HTTPS |
| Europa (Frankfurt) | eu-central-1 | inspector-scan.eu-central-1.amazonaws.com | HTTPS |
| Europa (Irlanda) | eu-west-1 | inspector-scan.eu-west-1.amazonaws.com | HTTPS |
| Europa (Londres) | eu-west-2 | inspector-scan.eu-west-2.amazonaws.com | HTTPS |

| Nome da região | Região | Endpoint | Protocolo |
| --- | --- | --- | --- |
| Europa (Milão) | eu-south-1 | inspector-scan.eu-south-1.amazonaws.com | HTTPS |
| Europa (Paris) | eu-west-3 | inspector-scan.eu-west-3.amazonaws.com | HTTPS |
| Europa (Estocolmo) | eu-north-1 | inspector-scan.eu-north-1.amazonaws.com | HTTPS |
| Europa (Zurique) | eu-central-2 | inspector-scan.eu-central-2.amazonaws.com | HTTPS |
| Oriente Médio (Barém) | me-south-1 | inspector-scan.me-south-1.amazonaws.com | HTTPS |
| América do Sul (São Paulo) | sa-east-1 | inspector-scan.sa-east-1.amazonaws.com | HTTPS |
| AWS GovCloud (Leste dos EUA) | us-gov-east-1 | digitalização do inspetor. us-gov-east-1.amazonaws.com<br><br>inspector-scan-fips. us-gov-east-1.amazonaws.com | HTTPS |

| Nome da região | Região | Endpoint | Protocolo |
| --- | --- | --- | --- |
| AWS GovCloud (Oeste dos EUA) | us-gov-west-1 | digitalização do inspetor. us-gov-west-1.amazonaws.com<br><br>inspector-scan-fips. us-gov-west-1.amazonaws.com | HTTPS |

# Disponibilidade de recursos específicos da região

Esta seção descreve a disponibilidade dos atributos do Amazon Inspector por Região da AWS.

Verificação do EC2 sem agente para regiões do Amazon EC2

A tabela a seguir mostra Regiões da AWS onde a digitalização sem agente para o Amazon EC2 está disponível atualmente.

| Nome da região | Código da região |
| --- | --- |
| Leste dos EUA (Norte da Virgínia) | us-east-1 |
| Oeste dos EUA (Oregon) | us-west-2 |
| Europa (Irlanda) | eu-west-1 |

Regiões de escaneamento de código do Lambda

A tabela a seguir mostra Regiões da AWS onde a digitalização de código Lambda está disponível atualmente.

| Nome da região | Código da região |
| --- | --- |
| Leste dos EUA (Norte da Virgínia) | us-east-1 |
| Oeste dos EUA (Oregon) | us-west-2 |

| Nome da região | Código da região |
| --- | --- |
| Leste dos EUA (Ohio) | us-east-2 |
| Ásia-Pacífico (Sydney) | ap-southeast-2 |
| Ásia-Pacífico (Tóquio) | ap-northeast-1 |
| Europa (Frankfurt) | eu-central-1 |
| Europa (Irlanda) | eu-west-1 |
| Europa (Londres) | eu-west-2 |
| Europa (Estocolmo) | eu-north-1 |
| Ásia-Pacífico (Singapura) | ap-southeast-1 |

### AWS GovCloud (US) Regiões

Para obter as informações mais recentes, consulte Amazon Inspector no Guia do usuário do AWS GovCloud (US) .

# Histórico do documento para o Guia do usuário do Amazon Inspector

A tabela a seguir descreve as alterações importantes na documentação desde a última versão do Amazon Inspector. Para receber notificações sobre atualizações dessa documentação, você poderá se inscrever em um feed RSS.

| Alteração | Descrição | Data |
| --- | --- | --- |
| Funcionalidade atualizada | O Amazon Inspector atualiza o período de retenção para descobertas fechadas de 30 dias para 7 dias. Para obter mais informações, consulte Entendendo as descobertas no Amazon Inspector. | 12 de fevereiro de 2024 |
| Funcionalidade atualizada | O Amazon Inspector adicionou uma nova declaração à política do AmazonInspector2ServiceRolePolicy. A nova declaração permite que o Amazon Inspector inicie escaneamentos CIS para sua instância. | 23 de janeiro de 2024 |
| Nova política | O Amazon Inspector adicionou uma nova política, AmazonInspector2ManagedCisPolicypolítica, que você pode usar como parte de um perfil de instância para permitir escaneamentos do CIS em uma instância. | 23 de janeiro de 2024 |
| Novo recurso | O Amazon Inspector agora atualizará a duração da nova | 23 de janeiro de 2024 |

| | | |
|---|---|---|
| | digitalização do ECR das imagens do contêiner quando você as extrair. Para alterar a duração da nova verificação com base nas datas de envio ou recebimento, consulte Configuração da duração da nova verificação do ECR. | |
| Novo recurso | O Amazon Inspector agora pode executar escaneamentos do Center for Internet Security (CIS) em instâncias do EC2. Para obter mais informações, consulte Escaneamentos CIS do Amazon Inspector. | 23 de janeiro de 2024 |
| Novo recurso | Agora, o Amazon Inspector pode verificar imagens de contêiner em pipelines de CI/CD. Para obter mais informações, consulte Integração de CI/CD usando Amazon Inspector. | 30 de novembro de 2023 |
| Nova política | O Amazon Inspector adicionou uma nova política que permite que o Amazon Inspector verifique snapshots do Amazon EBS da instância do EC2 para verificação sem agente. Para obter mais informações sobre a política, consulte Verificação sem agente. | 27 de novembro de 2023 |

| | | |
|---|---|---|
| Novo recurso | Agora, o Amazon Inspector é compatível com a verificação de instâncias Amazon EC2 Linux sem a necessidade de agentes SSM por meio da varredura sem agente. Para obter mais informações, consulte Verificação sem agente. | 27 de novembro de 2023 |
| Novos recursos com suporte | O Amazon Inspector agora dá suporte a verificação de instâncias MacOS do Amazon EC2. Consulte Sistemas operacionais com suporte: ao escaneamento do Amazon EC2 para versões com suporte do MacOS. | 5 de outubro de 2023 |
| Novas regiões | O Amazon Inspector agora está disponível na Ásia-Pacífico (Jacarta), África (Cidade do Cabo), Asia Pacific (Osaka) e Europa (Zurique). | 29 de setembro de 2023 |
| Novo atributo | Agora você poderá excluir as instâncias do EC2 das verificações do Amazon Inspector usando tags de exclusão. | 14 de setembro de 2023 |

| | | |
|---|---|---|
| Novo recurso | O Amazon Inspector adicionou novas permissões que permitem que o Amazon Inspector verifique as configurações de rede das instâncias do Amazon EC2 que fazem parte dos grupos-alvo do Elastic Load Balancing. | 31 de agosto de 2023 |
| Novo atributo | O Amazon Inspector agora fornece detalhes de inteligência de vulnerabilidade para descobertas de vulnerabilidades de pacotes. | 31 de julho de 2023 |
| Funcionalidade atualizada | O Amazon Inspector adicionou novas permissões que permitem que usuários somente para leitura exportem a SBOM (Lista de Materiais de Software) para seus recursos. | 29 de junho de 2023 |
| Novo atributo | Agora você poderá exportar o SBOM para recursos que estão sendo verificados pelo Amazon Inspector. | 13 de junho de 2023 |

| | | |
|---|---|---|
| Novo atributo | O Escaneamento de código do Lambda agora está disponível ao público. Foram adicionados novos atributos que permitem criptografar o código identific ado em suas descobertas de escaneamento de código do Lambda. Além disso, o escaneamento de código do Lambda agora fornece sugestões de nova gravações de correção do seu código. | 13 de junho de 2023 |
| Funcionalidade atualizada | O Amazon Inspector adicionou uma nova declaração à política do AmazonIns pector2ReadOnlyAccess. As novas declarações permitem que usuários somente para leitura recuperem detalhes do status e das descobertas da verificação do código do Lambda em suas contas. | 2 de maio de 2023 |
| Novo recurso | O Amazon Inspector adicionou a Pesquisa de banco de dados de vulnerabilidades, que permite verificar se o Amazon Inspector cobre uma CVE específica. | 1º de maio de 2023 |

| | | |
|---|---|---|
| Funcionalidade atualizada | O Amazon Inspector adicionou novas permissões à AmazonInspector2ServiceRolePolicypolítica que permitem que o Amazon Inspector AWS CloudTrail crie canais vinculados a serviços em sua conta quando você ativa a digitalização Lambda. Isso permite que o Amazon Inspector monitore CloudTrail eventos em sua conta. | 30 de abril de 2023 |
| Funcionalidade atualizada | O Amazon Inspector adicionou uma nova declaração à política do AmazonInspector2FullAccess. A nova declaração permite que os usuários recuperem detalhes das descobertas de vulnerabilidade de código do escaneamento de código do Lambda. | 17 de abril de 2023 |
| Funcionalidade atualizada | O Amazon Inspector adicionou uma nova declaração à política do AmazonInspector2ServiceRolePolicy. A nova declaração permite que o Amazon Inspector envie informações ao Amazon EC2 Systems Manager sobre os caminhos personalizados que você definiu para a inspeção profunda do Amazon EC2. | 17 de abril de 2023 |

| | | |
|---|---|---|
| Novo recurso | O Amazon Inspector adiciona suporte adicional para instâncias Linux EC2 na forma de inspeção profunda do Amazon Inspector, que verifica suas instâncias em busca de vulnerabilidades de pacotes em pacotes de linguagem de programação de aplicativos. | 17 de abril de 2023 |
| Funcionalidade atualizada | O Amazon Inspector adicionou uma nova declaração à política do AmazonInspector2ServiceRolePolicy. As novas declarações permitem que o Amazon Inspector solicite escaneamentos do código do desenvolvedor em AWS Lambda funções e receba dados de escaneamento da Amazon Security. CodeGuru Além disso, o Amazon Inspector adicionou permissões para examinar as políticas do IAM. O Amazon Inspector usa essas informações para verificar as vulnerabilidades do código nas funções do Lambda. | 28 de fevereiro de 2023 |

| | | |
|---|---|---|
| Novo recurso | O Amazon Inspector adiciona suporte adicional para funções do Lambda na forma de Escaneamento de código do Lambda, que verifica o código do desenvolvedor de suas funções do Lambda em busca de vulnerabilidades de segurança. | 28 de fevereiro de 2023 |
| Funcionalidade atualizada | O Amazon Inspector adicionou uma nova declaração à política do AmazonInspector2ServiceRolePolicy. A nova declaração permite que o Amazon Inspector recupere informações CloudWatch sobre quando uma AWS Lambda função foi invocada pela última vez. Usa essas informações para focar as varreduras nas funções Lambda em seu ambiente que estiveram ativas nos últimos 90 dias. | 20 de fevereiro de 2023 |

| | | |
|---|---|---|
| Funcionalidade atualizada | O Amazon Inspector adicionou uma nova declaração à política do AmazonInspector2ServiceRolePolicy. A nova declaração permite que o Amazon Inspector recupere informações sobre suas funções do AWS Lambda . O Amazon Inspector usa essas informações para verificar se há vulnerabilidades de segurança nas funções do Lambda. | 28 de novembro de 2022 |
| Novo recurso | O Amazon Inspector adiciona suporte para funções de digitalização AWS Lambda. | 28 de novembro de 2022 |
| Conteúdo atualizado | Foram adicionados procedimentos, exemplos de políticas e dicas para exportar relatórios de descobertas do Amazon Inspector para um bucket do Amazon Simple Storage Service (Amazon S3). | 14 de outubro de 2022 |
| Novo conteúdo | Foram adicionadas informações sobre a avaliação da cobertura do AWS seu ambiente pelo Amazon Inspector usando o console do Amazon Inspector. As informações incluem descrições dos valores de Status para recursos individuais em seu ambiente. | 7 de outubro de 2022 |

| | | |
|---|---|---|
| Novo recurso | O Amazon Inspector agora fornece detalhes adicionais sobre como corrigir vulnerabilidades de pacotes. Novos campos foram adicionados para detalhes da descoberta Os novos campos fornecem contexto sobre se uma correção está disponível por meio de uma atualização de pacote. Se uma correção estiver disponível, a seção Correção sugerida de uma descoberta mostra os comandos que você poderá executar para fazer a correção. | 2 de setembro de 2022 |
| Funcionalidade atualizada | O Amazon Inspector adicionou uma nova declaração à política do AmazonInspector2ServiceRolePolicy. A nova ação permite que o Amazon Inspector descreva as execuções da associação do SSM. O Amazon Inspector também adicionou um escopo adicional de recursos para permitir que o Amazon Inspector crie, atualize, exclua e inicie associações de SSM com documentos do SSM de propriedade do `AmazonInspector2` . | 31 de agosto de 2022 |

| | | |
|---|---|---|
| Novo recurso | O Amazon Inspector agora dá suporta verificações de instâncias do Windows. O Amazon Inspector agora poderá verificar instância s gerenciadas por SSM executando sistemas operacionais com suporte pelo Windows. As varredura s de Windows hosts são realizadas pelo plug-in Amazon Inspector SSM, que é instalado e invocado por meio de novas associações de SSM criadas automaticamente pelo Amazon Inspector. | 31 de agosto de 2022 |
| Funcionalidade atualizada | O Amazon Inspector atualizou o escopo dos recursos da AmazonInspector2ServiceRole Policypolítica para permitir que o Amazon Inspector colete inventário de software em outras partições. AWS | 12 de agosto de 2022 |
| Funcionalidade atualizada | Na política do AmazonIns pector2ServiceRolePolicy, o Amazon Inspector estruturo u novamente o escopo dos recursos das ações, permitindo que o Amazon Inspector crie, exclua e atualize associações de SSM. | 10 de agosto de 2022 |

| | | |
|---|---|---|
| Novo recurso | O Amazon Inspector agora dá suporte a alteração da configuração de duração da nova verificação automática do ECR. A configuração de duração da nova verificação automática do Amazon ECR determina por quanto tempo o Amazon Inspector monitora continuamente as imagens enviadas para os repositór ios. Quando uma imagem é mais antiga do que a duração da verificação, o Amazon Inspector não verifica mais a imagem e fecha todas as descobertas existentes para ela. Todas as novas contas terão automaticamente a duração da nova verificação automática do ECR definida como vitalícia. As contas criadas anteriormente tinham uma duração de nova verificaç ão automática do ECR de 30 dias, mas agora você pode escolher entre 30 dias, 180 dias ou durações vitalícias para as verificações. | 25 de junho de 2022 |

| | | |
|---|---|---|
| Nova funcionalidade | O Amazon Inspector adicionou uma nova política AWS gerenciada, a AmazonInspector2ReadOnlyAccesspolítica, para permitir acesso somente de leitura à funcionalidade do Amazon Inspector. | 21 de janeiro de 2022 |
| Disponibilidade geral | Essa é o lançamento inicial público do Guia do usuário do Amazon Inspector. | 29 de novembro de 2021 |

# AWS Glossário

Para obter a AWS terminologia mais recente, consulte o AWS glossário na Glossário da AWS Referência.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.