Manual do usuário

Amazon Inspector Classic

Versão Latest

Amazon Inspector Classic: Manual do usuário

Table of Contents

Este é o manual do usuário do Amazon Inspector Classic. Para obter informações sobre o novo Amazon Inspector, consulte o Guia do usuário do Amazon Inspector. Para acessar o console do Amazon Inspector Classic, abra o console do Amazon Inspector em https://console.aws.amazon.com/inspector/ e escolha Amazon Inspector Classic no painel de navegação.

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.

O que é o Amazon Inspector Classic?

> **Note**
>
> O novo Amazon Inspector, uma versão completamente reformulada e redesenhada do Amazon Inspector Classic, está agora disponível em todo o Regiões da AWS. O novo Amazon Inspector expandiu a cobertura para adicionar suporte para imagens de contêineres residentes no Amazon Elastic Container Registry (Amazon ECR), além de instâncias EC2. O novo Amazon Inspector oferece suporte a várias contas por meio de integração e verificação contínua de vulnerabilidades de software e acessibilidade de rede com AWS Organizations base em vulnerabilidades e exposições comuns (CVEs). Incentivamos você a explorar e usar esses e outros recursos novos e aprimorados e a se beneficiar do valor de segurança significativamente aprimorado. Para saber mais sobre os recursos e preços do novo Amazon Inspector, consulte Amazon Inspector. Para saber como mover para o novo Amazon Inspector, consulte Mudando para o novo Amazon Inspector.

O Amazon Inspector Classic testa a acessibilidade da rede das instâncias do Amazon EC2 e o estado da segurança das aplicações executadas nessas instâncias. O Amazon Inspector Classic avalia os aplicativos quanto à exposição, vulnerabilidades e desvios das práticas recomendadas. Depois de fazer uma avaliação, o Amazon Inspector Classic gera uma lista detalhada dos problemas de segurança encontrados por nível de gravidade.

Com o Amazon Inspector Classic, você pode automatizar avaliações de vulnerabilidade de segurança por todo o seu pipeline de desenvolvimento e implantação ou para sistemas de produção estáticos. Isso permite que você faça testes de segurança de uma parte regular de desenvolvimento e operações de TI.

O Amazon Inspector Classic oferece software predefinido chamado de agente que você pode instalar no sistema operacional das instâncias do EC2 que você deseja avaliar. O agente monitora o comportamento das instâncias EC2, incluindo a rede, o sistema de arquivos e a atividade do processo. Ele também coleta um amplo conjunto de dados de comportamento e configuração (telemetria).

Important

AWS não garante que seguir as recomendações fornecidas resolva todos os possíveis problemas de segurança. As descobertas geradas pelo Amazon Inspector Classic dependem da sua escolha de pacotes de regras incluídos em cada modelo de avaliação, da presença de não AWS componentes em seu sistema e de outros fatores. Você é responsável pela segurança dos aplicativos, processos e ferramentas executados nos AWS serviços. Para obter mais informações, consulte o Modelo de responsabilidade compartilhada do AWS para a segurança.

Note

AWS é responsável por proteger a infraestrutura global que executa os serviços oferecidos na AWS nuvem. Essa infraestrutura consiste em hardware, software, rede e instalações que executam AWS serviços. AWS fornece vários relatórios de auditores terceirizados que verificaram nossa conformidade com uma variedade de normas e regulamentações de segurança de computadores. Para obter mais informações, consulte Conformidade da Nuvem AWS.

Para obter informações sobre a terminologia do Amazon Inspector Classic, consulte Terminologia e conceitos do Amazon Inspector Classic.

Benefícios do Amazon Inspector Classic

Aqui estão alguns dos principais benefícios do Amazon Inspector Classic:

- Integre verificações de segurança automatizadas em seus processos regulares de implantação e produção — Avalie a segurança de seus AWS recursos para fins forenses, de solução de problemas ou de auditoria ativa. Execute as avaliações durante o processo de desenvolvimento ou execute-os em um ambiente de produção estável.
- Encontre problemas de segurança do aplicativo – Automatize a avaliação de segurança dos seus aplicativos e identifique proativamente vulnerabilidades. Isso permite que você desenvolva e itere novos aplicativos rapidamente e avalie a conformidade com as práticas recomendadas e políticas.

- Obtenha uma compreensão mais profunda de seus AWS recursos — Mantenha-se informado sobre os dados de atividade e configuração de seus AWS recursos analisando as descobertas que o Amazon Inspector Classic produz.

Recursos do Amazon Inspector Classic

Aqui estão alguns dos principais recursos do Amazon Inspector Classic:

- Verificação de configuração e mecanismo de monitoramento de atividade – O Amazon Inspector Classic fornece um agente que analisa o sistema e a configuração do recurso. Ele também monitora a atividade para determinar a aparência de uma meta, como ele se comporta e seus componentes dependentes. A combinação dessa telemetria fornece uma visão completa da meta e seus possíveis problemas de segurança ou de conformidade.
- Biblioteca de conteúdo integrado – O Amazon Inspector Classic, inclui uma biblioteca integrada de regras e relatórios. Isso inclui verificações com base em melhores práticas, padrões de conformidade comuns e vulnerabilidades. Essas verificações incluem etapas recomendadas detalhadas para resolver potenciais problemas de segurança.
- Automação por meio de uma API – O Amazon Inspector Classic pode ser totalmente automatizado por uma API. Isso permite incorporar testes de segurança no processo de desenvolvimento e design, incluindo a seleção de relatórios, a execução e o fornecimento dos resultados desses testes.

Acessando o Amazon Inspector Classic

Você pode trabalhar com o serviço Amazon Inspector Classic de qualquer uma das seguintes formas:

Console do Amazon Inspector Classic

Faça login AWS Management Console e abra o console do Amazon Inspector Classic em https://console.aws.amazon.com/inspector/.

O console é uma interface baseada em navegador que permite acesso e uso do serviço do Amazon Inspector Classic.

AWS SDKs

AWS fornece kits de desenvolvimento de software (SDKs) que consistem em bibliotecas e exemplos de código para várias linguagens e plataformas de programação. Eles incluem Java, Python, Ruby, .NET, iOS, Android e muito mais. Os SDKs fornecem uma forma conveniente para criar acesso programático ao serviço Amazon Inspector Classic. Para obter informações sobre os AWS SDKs, incluindo como baixá-los e instalá-los, consulte Tools for Amazon Web Services.

API HTTPS do Amazon Inspector Classic

Você pode acessar o Amazon Inspector Classic e AWS programaticamente usando a API HTTPS do Amazon Inspector Classic, que permite emitir solicitações HTTPS diretamente para o serviço. Para obter mais informações, consulte a Referência de API do Amazon Inspector Classic.

AWS Ferramentas de linha de comando

Você pode usar as ferramentas de linha de AWS comando para executar comandos na linha de comando do seu sistema para realizar tarefas do Amazon Inspector Classic. As ferramentas de linha de comando também são úteis se você quiser criar scripts que executem AWS tarefas. Para obter mais informações, consulte a interface de linha de AWS comando do Amazon Inspector Classic.

Terminologia e conceitos do Amazon Inspector Classic

Ao começar a usar o Amazon Inspector Classic, você pode se beneficiar com o aprendizado dos seus conceitos principais.

Agente do Amazon Inspector Classic

Um agente de software que você pode instalar nas instâncias do EC2 incluídas no destino de avaliação. O agente coleta um amplo conjunto de dados de configuração (telemetria). Para obter mais informações, consulte Agentes do Amazon Inspector Classic.

Execução de avaliação

O processo de descoberta de possíveis problemas de segurança por meio da análise da configuração do destino de avaliação em relação aos pacotes de regras especificados. Durante uma execução de avaliação, o Amazon Inspector monitora, coleta e analisa dados de configuração (telemetria) de recursos na meta especificada. Depois, o Amazon Inspector analisa os dados e os compara com um conjunto de pacotes de regras de segurança especificados no modelo de avaliação durante a execução da avaliação. Uma execução de avaliação completa

gera uma lista de descobertas, que inclui os possíveis problemas de segurança com diferentes graus de severidade. Para obter mais informações, consulte Modelos de avaliação e execuções de avaliação do Amazon Inspector Classic.

Destino de avaliação

No contexto do Amazon Inspector Classic, um conjunto de recursos da AWS que funcionam juntos como uma unidade para ajudar você a atingir seus objetivos empresariais. O Amazon Inspector Classic avalia o estado da segurança dos recursos que constituem o destino de avaliação.

> **Important**
>
> No momento, os destinos de avaliação do Amazon Inspector Classic podem consistir somente em instâncias do EC2. Para obter mais informações, consulte Limites do serviço do Amazon Inspector Classic.

Para criar um destino de avaliação do Amazon Inspector Classic, primeiro você deve marcar suas instâncias do EC2 com os pares de chave e valor de sua escolha. Em seguida, você pode criar uma exibição dessas instâncias do EC2 marcadas que têm chaves ou valores comuns. Para obter mais informações, consulte Destinos de avaliação do Amazon Inspector Classic.

Modelo de avaliação

A configuração que é usada durante a execução de avaliação. O modelo inclui o seguinte:

- Pacote de regras que o Amazon Inspector Classic usa para avaliar o destino de avaliação
- Tópicos do Amazon SNS para os quais você deseja que o Amazon Inspector Classic envie notificações sobre estados de execução de avaliação e descobertas
- Tags (pares de chave e valor) que você pode atribuir a descobertas que são geradas pela execução de avaliação
- A duração da execução de avaliação

Descoberta

Um possível problema de segurança que o Amazon Inspector Classic descobre durante uma execução de avaliação da meta especificada. As descobertas são exibidas no console do Amazon Inspector Classic ou recuperadas por meio da API. Elas contêm uma descrição detalhada do problema de segurança e uma recomendação sobre como corrigi-lo. Para obter mais informações, consulte Descobertas do Amazon Inspector Classic.

Regra

No contexto do Amazon Inspector Classic, uma verificação de segurança realizada durante uma execução de avaliação. Quando uma regra detecta um possível problema de segurança, o Amazon Inspector Classic gera uma descoberta que descreve o problema.

Pacote de regras

No contexto do Amazon Inspector Classic, uma coleção de regras. Um pacote de regras corresponde a um objetivo de segurança que você possa ter. Você pode especificar o objetivo de segurança selecionando o pacote de regras apropriado ao criar um modelo de avaliação do Amazon Inspector Classic. Para obter mais informações, consulte Pacotes de regras e regras do Amazon Inspector Classic.

Telemetria

Informações de pacotes instalados e configuração de software para uma instância do EC2. O Amazon Inspector Classic coleta os dados durante uma execução de avaliação.

Limites do serviço do Amazon Inspector Classic

A tabela a seguir mostra os limites do Amazon Inspector Classic para uma conta da AWS.

> **Important**
>
> No momento, os destinos de avaliação podem consistir somente de instâncias do EC2.

Veja a seguir os limites do Amazon Inspector Classic por conta da AWS, por região:

Recurso	Limite padrão	Comentários
Instâncias em avaliações em execução	500	O número máximo de instâncias do EC2 que podem ser incluídas em todas as avaliações em execução por conta, por região.

Recurso	Limite padrão	Comentários
Execuções de avaliação	50000	O número máximo de execuções de avaliação que podem ser criadas por conta por região. Você pode ter várias execuções de avaliação acontecendo ao mesmo tempo, desde que os destinos de avaliação usados para essas execuções não tenham sobreposição de instâncias do EC2.
Modelos de avaliação	500	O número máximo de modelos de avaliação que você pode ter em um determinado momento por conta, por região.
Destinos de avaliação	50	O número máximo de destinos de avaliação que você pode ter em um determinado momento por conta, por região.

Salvo indicação em contrário, esses limites podem ser aumentados mediante solicitação contatando aCentral da AWS Support.

Preços do Amazon Inspector Classic

A definição de preços do Amazon Inspector Classic é baseada no número de instâncias do EC2 incluídas em cada avaliação e nos pacotes de regras usados nessas avaliações.

Preços do pacote de regras de acessibilidade da rede

As avaliações do Amazon Inspector Classic com os pacotes de regras de acessibilidade da rede são cobradas por instância, por avaliação (avaliação de instância) por mês. Por exemplo, se você executar 1 avaliação em relação a 1 instância, isso será 1 avaliação de instância. Se você executar 1 avaliação em 10 instâncias, serão 10 avaliações de instância. O preço começa em 0,15 USD por avaliação de instância por mês, com descontos por volume até chegar a 0,04 USD por avaliação de instância por mês.

Detalhes do teste gratuito

Primeiros 90 dias usando o Amazon Inspector Classic	Preço de avaliação por instância
Primeiras 250 avaliações de instância	$0,00

Detalhes de preço

Em um determinado mês	Preço de avaliação por instância
Primeiras 250 avaliações de instância	0,15 US$
Próximas 750 avaliações de instância	0,13 US$
Próximas 4.000 avaliações de instância	0,10 USD
Próximas 45.000 avaliações de instância	$0,07
Todas as outras avaliações de instância	$0,04

Preços dos pacotes de regras de avaliação de hosts

Para qualquer combinação de vulnerabilidades e exposições comuns (CVE), benchmarks do Center for Internet Security (CIS), práticas recomendadas de segurança e análise de comportamento de runtime incluída nas avaliações

Os pacotes de regras de avaliação de host do Amazon Inspector Classic usam um agente implantado nas instâncias do Amazon EC2 que executam os aplicativos que você deseja avaliar. As avaliações com os pacotes de regras de host são cobradas por agente por avaliação (avaliação do agente) por mês. Por exemplo, se você executar 1 avaliação em relação a 1 agente, isso é 1 avaliação de agente. Se você executar 1 avaliação contra 10 agentes, são 10 avaliações de agentes. O preço começa em 0,30 USD por avaliação de agente por mês, com descontos por volume até chegar a 0,05 USD por avaliação de agente por mês.

Detalhes do teste gratuito

Primeiros 90 dias usando o Amazon Inspector Classic	Preço por avaliação do agente
Primeiras 250 avaliações de agentes	$0,00

Detalhes de preço

Em um determinado mês	Preço por avaliação do agente
Primeiras 250 avaliações de agentes	$0,30
Próximas 750 avaliações de agentes	$0,25
Próximas 4.000 avaliações de agentes	0,15 US$
Próximas 45.000 avaliações de agentes	0,10 USD
Todas as outras avaliações de agentes	0,05 USD

Sistemas operacionais e regiões compatíveis com o Amazon Inspector Classic

Esse capítulo fornece informações sobre os sistemas operacionais e regiões da AWS com as quais o Amazon Inspector Classic é compatível.

> **Important**
>
> No momento, os destinos de avaliação do Amazon Inspector Classic podem consistir somente em instâncias do EC2. Você pode executar uma avaliação sem agente com o pacote de regras Acessibilidade de rede em qualquer instância do EC2, independentemente do sistema operacional.

Para obter informações sobre os pacotes de regras do Amazon Inspector Classic que estão disponíveis entre sistemas operacionais compatíveis, consulte Pacotes de regras do Amazon Inspector Classic para sistemas operacionais compatíveis.

Tópicos

Sistemas operacionais baseado em Linux compatíveis com o agente do Amazon Inspector Classic

Você pode usar o agente do Amazon Inspector Classic em instâncias de 64-bit x86 e Arm EC2. O agente é compatível com as seguintes versões dos sistemas operacionais baseados em Linux:

- Instâncias de 64-bit x86
  - Amazon Linux 2
  - Amazon Linux (2018.03, 2017.09, 2017.03, 2016.09, 2016.03, 2015.09, 2015.03, 2014.09, 2014.03, 2013.09, 2013.03, 2012.09, 2012.03)
  - Ubuntu (20.04 LTS, 18.04 LTS, 16.04 LTS, 14.04 LTS)

  - Debian (10.x, 9.0 - 9.5, 8.0 - 8.7)
  - Red Hat Enterprise Linux (8.x, 7.2 - 7.x, 6.2 - 6.9)
  - CentOS (7.2 - 7.X, 6.2 - 6.9)
- Instâncias Arm
  - Amazon Linux 2
  - Red Hat Enterprise Linux (7.6 - 7.x)
  - Ubuntu (18.04 LTS, 16.04 LTS)

Sistemas operacionais baseados no Windows compatíveis com o agente Amazon Inspector Classic

Você só pode usar o agente do Amazon Inspector Classic em instâncias do EC2 que executam a versão de 64 bits dos seguintes sistemas operacionais Windows:

- Windows Server 2019 Base
- Windows Server 2016 Base
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Regiões da AWS compatíveis

O Amazon Inspector Classic é compatível nas seguintes regiões da AWS:

- Leste dos EUA (Ohio) us-east-2
- Leste dos EUA (Norte da Virgínia) us-east-1
- Oeste dos EUA (Norte da Califórnia) us-west-1
- Oeste dos EUA (Oregon) us-west-2
- Ásia-Pacífico (Mumbai) ap-south-1
- Ásia-Pacífico (Seul) ap-northeast-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
- AWS GovCloud (Leste dos EUA) -1 gov-us-east
- AWS GovCloud (Oeste dos EUA) -1 gov-us-west

> **Note**
>
> O pacote de regras de acessibilidade de rede não está disponível nas regiões AWS GovCloud (EUA).

Mudando para o novo Amazon Inspector

O novo Amazon Inspector agora está disponível globalmente em Regiões da AWS. O novo Amazon Inspector é uma versão completamente rearquitetada e redesenhada do Amazon Inspector existente, agora chamado de Amazon Inspector Classic. Os seguintes recursos são os principais aprimoramentos do Amazon Inspector:

- Construído para escala — O novo Amazon Inspector foi criado para escala e o ambiente dinâmico da nuvem. Não há limite para o número de instâncias ou imagens que podem ser digitalizadas em uma conta.
- Suporte para imagens de contêineres — O novo Amazon Inspector também escaneia imagens de contêineres residentes no Amazon Elastic Container Registry (Amazon ECR) em busca de vulnerabilidades de software.
- Suporte para gerenciamento de várias contas — O novo Amazon Inspector é integrado a Organizações. Isso permite que você delegue uma conta de administrador para o Amazon Inspector da sua organização. A conta de administrador delegado é uma conta centralizada que consolida todas as descobertas e pode configurar todas as contas dos membros.
- AWS Systems Manager Agente de Usa (Agente SSM) — Com o novo Amazon Inspector, você não precisa mais instalar e manter um agente autônomo do Amazon Inspector em todas as suas instâncias do EC2. O novo Amazon Inspector aproveita o agente SSM amplamente implantado.
- Verificação automática e contínua — Com o Amazon Inspector Classic, você configura manualmente os destinos, os modelos e a frequência das avaliações. No entanto, a nova versão do Amazon Inspector detecta automaticamente todas as instâncias do EC2 recém-lançadas e imagens de contêineres elegíveis enviadas ao Amazon ECR e as examina imediatamente em busca de vulnerabilidades de software e exposição não intencional na rede. Os recursos são automaticamente digitalizados novamente com base em vários gatilhos, incluindo uma nova instância do EC2 sendo lançada, uma imagem de contêiner sendo enviada para o Amazon ECR, a instalação de um novo pacote em uma instância do EC2, a instalação de um patch ou a publicação de uma nova Common Vulnerabilities and Exposure (CVE) que afeta o recurso.
- Pontuação de risco do Amazon Inspector — O novo Amazon Inspector calcula uma pontuação de risco do Amazon Inspector para ajudar a priorizar suas descobertas. A pontuação de risco é calculada correlacionando as informações do up-to-date CVE com fatores temporais e ambientais, como acessibilidade da rede e informações de explorabilidade.
- Mais integrações — Todas as descobertas são agregadas em um console recém-projetado do Amazon Inspector e enviadas para AWS Security Hub a Amazon para automatizar fluxos de

trabalho, como emissão de tíquetes. EventBridge As descobertas relacionadas à imagem do contêiner também são enviadas ao Amazon ECR.

Para saber mais sobre todos os recursos e preços do novo Amazon Inspector, consulte o Guia do usuário do Amazon Inspector.

Embora continuemos a oferecer suporte ao Amazon Inspector Classic por algum tempo e os clientes possam usar o novo Amazon Inspector e o Amazon Inspector Classic na mesma conta, recomendamos que você migre para o novo Amazon Inspector. As seções a seguir mostram o processo de migração do Amazon Inspector Classic para o novo Amazon Inspector.

Tópicos

Etapa 1: (opcional) exportar relatórios de avaliação e resultados

Para salvar os relatórios de avaliação e as descobertas no Amazon Inspector Classic, gere um relatório de avaliação.

Para gerar um relatório de avaliação

1. Na página Execuções de avaliação, localize a execução de avaliação para a qual você deseja gerar um relatório. Certifique-se de que seu status é Análise completa.
2. Na coluna Relatórios dessa execução de avaliação, selecione o ícone de relatórios.

   > **Important**
   >
   > O ícone de relatórios está presente na coluna Relatórios somente para as execuções de avaliação que ocorreram ou vão ocorrer após 25 de abril de 2017. Essa é a data em que os relatórios de avaliação foram disponibilizados no Amazon Inspector Classic.

3. Na caixa de diálogo Relatório de avaliação, selecione o tipo de relatório que você deseja visualizar (um relatório de Descobertas ou um relatório Completo) e o formato do relatório (HTML ou PDF). Depois, escolha Gerar relatório.

Etapa 2: Excluir todas as execuções de avaliação programadas no Amazon Inspector Classic

Para desativar o Amazon Inspector Classic, exclua todos os modelos de avaliação em sua conta em todos os ativos Regiões da AWS. A exclusão de modelos de avaliação interrompe todas as futuras execuções de avaliação programadas.

Para excluir um modelo de avaliação

- Na página Modelos de avaliação, selecione o modelo que você deseja excluir e selecione Excluir. Quando a confirmação for solicitada, selecione Sim.

> **Important**
>
> Ao excluir um modelo de avaliação, todas as execuções de avaliação, descobertas e versões dos relatórios associados a esse modelo também são excluídas.

Etapa 3: habilitar o novo Amazon Inspector

Você pode habilitar o novo Amazon Inspector usando as AWS Management Console ou as novas APIs do Amazon Inspector. Para começar a usar o novo Amazon Inspector, consulte Conceitos básicos no Guia do usuário do Amazon Inspector.

Conceitos básicos do Amazon Inspector Classic

Esse tutorial mostra como configurar o Amazon Inspector Classic e começar criando e executando a primeira avaliação.

Configuração com um clique

O procedimento a seguir mostra como criar e executar uma avaliação automática usando um modelo pré-construído e parâmetros de agendamento predefinidos (uma vez por semana ou apenas uma vez) em todas as instâncias disponíveis do Amazon Elastic Compute Cloud (Amazon EC2) no atual Conta da AWS e Região da AWS.

1. Faça login no AWS Management Console e abra o console do Amazon Inspector Classic em https://console.aws.amazon.com/inspector/.
2. Na página Welcome (Bem-vindo), escolha o tipo de avaliação que deseja executar. Avaliações de rede analisam as configurações de rede de seu ambiente AWS buscando por vulnerabilidades, e não precisam de um agente do Amazon Inspector Classic. Avaliações de host analisam o software no host e as configurações de suas instâncias do EC2 em busca de vulnerabilidades e exija que um agente seja instalado nas instâncias do EC2.

   Escolha Executar semanalmente (recomendado) ou Executar uma vez. Assim que fizer sua escolha, o serviço criará a avaliação para você de maneira automática. De forma mais específica, o serviço faz o seguinte:

   a. Cria uma função vinculada a serviço.

      > **Note**
      >
      > Para identificar as instâncias do EC2 especificadas nos alvos de avaliação, o Amazon Inspector Classic precisa enumerar as instâncias e tags do EC2. O Amazon Inspector Classic obtém acesso a esses recursos em seu Conta da AWS por meio de uma função vinculada ao serviço chamada `AWSServiceRoleForAmazonInspector`. Para obter mais informações sobre funções vinculadas a um serviço, consulte Uso de funções vinculadas a serviço para o Amazon Inspector Classic e Como usar funções vinculadas a serviços.

b. Se possível, instale um agente do Amazon Inspector Classic em todas as instâncias do EC2 disponíveis em sua Conta da AWS e região.

> **Note**
>
> O serviço instala um agente do Amazon Inspector Classic somente nas instâncias do EC2 que permitem Executar Comando. AWS Systems Manager Para usar essa opção, verifique se todas as instâncias do EC2 na Conta da AWS conta e Região da AWS região atuais têm o agente do SSM instalado e uma função do IAM que permita Executar Comando. Para obter mais informações, consulte Como instalar o agente em várias instâncias do EC2 usando o Executar Comando do Systems Manager.

c. Adiciona essas instâncias a um destino de avaliação.

d. Inclui o destino em um modelo de avaliação com um conjunto padronizado de pacotes de regras.

e. Executa a avaliação semanalmente ou somente uma vez, dependendo se você escolheu Executar semanalmente (recomendado) ou Executar uma vez.

3. Na caixa de diálogo Confirmação escolha OK. O Amazon Inspector Classic executa automaticamente sua avaliação.

Configuração avançada

O procedimento a seguir mostra como escolher instâncias específicas do Amazon EC2, pacotes de regras e parâmetros de programação para incluir em um modelo e destino de avaliação.

1. Na página Bem-vindo, escolha Configuração avançada.
2. Na página Definir um destino de avaliação, insira o nome do destino de avaliação.
3. Em Todas as instâncias, você pode manter a caixa de seleção escolhida para incluir todas instâncias EC2 em sua Conta da AWS e região no destino de avaliação. Se quiser escolher qual instância EC2 para incluir, desmarque a caixa de seleção Todas as instâncias e insira as tags Chave e Valor associadas ao destino das instâncias EC2. Para mais informações sobre marcação das instâncias do EC2, consulte Como marcar seus recursos do Amazon EC2.
4. Em Instalar agentes, você poderá manter a caixa de seleção marcada por padrão se as instâncias permitirem o Comando de execução do System Manager. O serviço instala um agente do Amazon Inspector Classic em todas as instâncias do EC2 no destino de avaliação que

permitem AWS Systems Manager. Para usar essa opção, verifique se todas as instâncias do EC2 na conta Conta da AWS e região Região da AWS atuais têm o agente do SSM instalado e uma função do IAM que permita Executar Comando. Para obter mais informações, consulte Como instalar o agente em várias instâncias do EC2 usando o Executar Comando do Systems Manager. Se quiser instalar o agente de forma manual, consulte Instalação de agentes do Amazon Inspector.

5. Escolha Next (Próximo).
6. Na página Definir um modelo de avaliação, insira o nome desse modelo.
7. Em Pacotes de regras, escolha os pacotes para incluir no modelo de avaliação. Para mais informações sobre pacotes de regras, consulte Regras e pacotes de regras do Amazon Inspector.
8. Em Duração, escolha por quanto tempo haverá execução da avaliação.
9. (Opcional) Em Programação de avaliação, você pode definir uma programação para execuções de avaliação recorrentes.
10. Escolha Next (Próximo).
11. Na página Análise, revise suas escolhas para o modelo e destino de avaliação. Se estiver satisfeito com a configuração, escolha Criar. Se você definir uma programação de avaliação para o modelo de avaliação, a avaliação é executada automaticamente após escolher Criar.

> **Note**
>
> Para identificar as instâncias do EC2 especificadas nos alvos de avaliação, o Amazon Inspector Classic precisa enumerar as instâncias e tags do EC2. O Amazon Inspector Classic obtém acesso a esses recursos em seu Conta da AWS por meio de uma função vinculada ao serviço chamada `AWSServiceRoleForAmazonInspector`. Para obter mais informações sobre o uso de funções vinculadas ao serviço no Amazon Inspector Classic, consulte Uso de funções vinculadas a serviço para o Amazon Inspector Classic. Para obter mais informações sobre funções vinculadas a serviços, consulte Usar funções vinculadas a serviços no Manual do usuário do AWS Identity and Access Management.

12. Se não tiver configurado uma programação de avaliação, navegue até o modelo de avaliação por meio do console e escolha Executar.

13. Para acompanhar o andamento da execução da avaliação, no painel de navegação do console, escolha Execuções de avaliação, e, em seguida, escolha Descobertas. Para mais informações sobre descobertas, consulte Descobertas do Amazon Inspector Classic.

Tutoriais do Amazon Inspector Classic

Os tutoriais a seguir mostram como realizar execuções de avaliação do Amazon Inspector Classic nos sistemas operacionais Ubuntu e Red Hat Enterprise Linux.

Tutoriais

- Tutorial: usando o Amazon Inspector Classic com o Red Hat Enterprise Linux
- Tutorial: usando o Amazon Inspector Classic com o Ubuntu Server

Tutorial do Amazon Inspector Classic - Red Hat Enterprise Linux

Antes de seguir as instruções deste tutorial, recomendamos que você se familiarize com o Terminologia e conceitos do Amazon Inspector Classic.

Este tutorial mostra como usar o Amazon Inspector Classic para analisar o comportamento de uma instância do EC2 que executa o sistema operacional Red Hat Enterprise Linux 7.5. Fornece instruções passo a passo sobre como navegar pelo fluxo de trabalho do Amazon Inspector Classic. O fluxo de trabalho inclui a preparação das instâncias do EC2 Amazon, executando um modelo de avaliação e realizando as correções de segurança recomendadas, geradas em descobertas da avaliação. Se você for um usuário iniciante e quiser configurar e executar uma avaliação do Amazon Inspector Classic com um clique, consulte Criação de uma avaliação básica.

Tópicos

- Etapa 1: configurar uma instância do Amazon EC2 para usar com o Amazon Inspector Classic
- Etapa 2: modificar sua instância do Amazon EC2
- Etapa 3: criar um destino de avaliação e instalar um agente na instância EC2
- Etapa 4: criar e executar o modelo de avaliação
- Etapa 5: localizar e analisar suas descobertas
- Etapa 6: aplicar a correção recomendada ao destino de avaliação.

Etapa 1: configurar uma instância do Amazon EC2 para usar com o Amazon Inspector Classic

Para este tutorial, crie uma instância EC2 que execute o Red Hat Enterprise Linux 7.5 e marque-a utilizando a chave Nome e um valor de **`InspectorEC2InstanceLinux`**.

> **Note**
>
> Para mais informações sobre a marcação de instâncias do EC2, consulte Recursos e tags.

Etapa 2: modificar sua instância do Amazon EC2

Para este tutorial, você modifica o destino da instância do EC2 para expô-lo ao possível problema de segurança CVE-2018-1111. Para mais informações, consulte https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1111 e Vulnerabilidades e exposições comuns

Conecte-se à sua instância, **`InspectorEC2InstanceLinux`**, e execute o comando a seguir:

```
sudo yum install dhclient-12:4.2.5-68.el7
```

Para obter instruções sobre como se conectar a uma instância do EC2, consulte Conectar à sua instância no Guia de usuário da Amazon EC2.

Etapa 3: criar um destino de avaliação e instalar um agente na instância EC2

O Amazon Inspector Classic usa destinos de avaliação para designar os recursos da AWS que você quer avaliar.

Para criar um destino de avaliação e instalar um agente na instância do EC2

1. Faça login no AWS Management Console e abra o console do Amazon Inspector Classic em https://console.aws.amazon.com/inspector/.
2. No painel de navegação, escolha Destinos de avaliação e, em seguida, Criar.

   Faça o seguinte:

   a. Em Nome, insira o nome do seu destino de avaliação.

Para este tutorial, insira **`MyTargetLinux`**.

b. Para Usar tags, escolha as instâncias do EC2 que você quer incluir no destino de avaliação, inserindo valores para os campos Chave e Valor.

   Para este tutorial, escolha a instância do EC2 que você criou na etapa anterior, inserindo **`Name`** no campo Chave e **`InspectorEC2InstanceLinux`** no campo Valor.

   Para incluir todas as instâncias do EC2 na conta da AWS e a região no destino de avaliação, marque a caixa Todas as instâncias.

c. Escolha Save (Salvar).

d. Instale um agente do Amazon Inspector Classic em sua instância do EC2 marcada. Para instalar um agente em todas as instâncias do EC2 incluídas em um destino de avaliação, marque a caixa Instalar agentes.

> **Note**
>
> Você também pode instalar o agente do Amazon Inspector Classic usando o Executar Comando do AWS Systems Manager. Para instalar o agente em todas as instâncias no destino de avaliação, você pode especificar as mesmas tags usadas para a criação do destino de avaliação. Ou você pode instalar o agente do Amazon Inspector Classic em sua instância do EC2 manualmente. Para obter mais informações, consulte Instalação de agentes do Amazon Inspector Classic.

e. Escolha Save (Salvar).

> **Note**
>
> Neste momento, o Amazon Inspector Classic cria uma função vinculada ao serviço chamada `AWSServiceRoleForAmazonInspector`. A função dá ao Amazon Inspector Classic o acesso necessário aos seus recursos. Para obter mais informações, consulte Criação de um perfil vinculado a serviço para Amazon Inspector Classic.

Etapa 4: criar e executar o modelo de avaliação

Para criar e executar seu modelo

1. No painel de navegação, escolha Assessment templates (Modelos de avaliação) e, depois, escolha Create (Criar).
2. Em Nome, insira o nome de seu modelo de avaliação. Para este tutorial, insira **`MyFirstTemplateLinux`**.
3. Em Nome do destino, escolha o destino de avaliação que você criou acima, **`MyTargetLinux`**.
4. Em Pacotes de regras, escolha os pacotes que você deseja usar neste modelo de avaliação.

   Para este tutorial, escolha Vulnerabilidades e exposições comuns-1.1.
5. Em Duração, especifique a duração do modelo de avaliação.

   Para este tutorial, selecione 15 minutos.
6. Escolha Criar e executar.

Etapa 5: localizar e analisar suas descobertas

Uma execução de avaliação concluída produz um conjunto de descobertas ou possíveis problemas de segurança que o Amazon Inspector Classic descobre no seu destino de avaliação. Você pode analisar as descobertas e seguir as etapas recomendadas para solucionar os possíveis problemas de segurança.

Neste tutorial, se você concluir as etapas anteriores, a execução da avaliação produzirá a descoberta sobre a vulnerabilidade comum CVE-2018-1111.

Para localizar e analisar sua descoberta

1. No painel de navegação, escolha Assessment runs (Execuções de avaliação). Verifique se o status da execução do modelo de avaliação chamado MyFirstTemplateLinux está definido como Coleta de dados. Isso indica que a execução da avaliação está atualmente em andamento e os dados da telemetria para sua meta estão sendo coletados e analisados em relação aos pacotes de regras selecionados.
2. Não é possível visualizar as descobertas geradas pela execução da avaliação enquanto ela ainda estiver em andamento. Deixe a demonstração executar totalmente por toda a duração. No entanto, para este tutorial, você pode interromper a execução após alguns minutos.

O status de MyFirstTemplateLinux muda primeiro para Interrupção, para Análise depois de alguns minutos e, finalmente, Análise concluída. Para ver essas alterações no status, escolha o ícone Atualizar.

3. No painel de navegação, selecione Descobertas.

Uma nova descoberta de severidade Alta chamada Instância InspectorEC2InstanceLinux é vulnerável a CVE-2018-1111.

> **Note**
>
> Se a nova descoberta não for exibida, selecione o ícone Atualizar.

Para expandir a exibição e ver os detalhes dessa descoberta, selecione a seta à esquerda da descoberta. Os detalhes da descoberta incluem o seguinte:

- ARN da descoberta
- Nome da execução da avaliação que produziu a descoberta
- Nome do destino de avaliação que produziu a descoberta
- Nome do modelo de avaliação que produziu a descoberta
- O horário de início da execução da avaliação
- O horário de término da execução da avaliação
- O status da execução da avaliação
- O nome do pacote de regras que inclui a regra que acionou a descoberta
- ID do agente do Amazon Inspector Classic
- O nome da descoberta
- A severidade da descoberta
- A descrição da descoberta
- Etapas de solução recomendadas que você pode concluir para corrigir o possível problema de segurança descrito pela descoberta

Etapa 6: aplicar a correção recomendada ao destino de avaliação.

Para este tutorial, você modificou o destino de avaliação para expô-lo a um possível problema de segurança CVE-2018-1111. Neste procedimento, você aplica a correção recomendada para esse problema.

Para aplicar a correção à sua meta

1. Conecte-se à instância **`InspectorEC2InstanceLinux`** que você criou na seção anterior e execute o seguinte comando:

   ```
   sudo yum update dhclient-12:4.2.5-68.el7
   ```

2. Na página Modelos de avaliação, escolha MyFirstTemplateLinux e, em seguida, escolha Executar para iniciar uma nova execução de avaliação usando este modelo.
3. Siga as etapas em Etapa 5: localizar e analisar suas descobertas para ver as descobertas que resultam dessa execução subsequente do modelo MyFirstTemplateLinux.

   Por ter solucionado o problema de segurança CVE-2018-1111, você não deve mais ver uma descoberta para ele.

Tutorial do Amazon Inspector Classic - Ubuntu Server

Antes de seguir as instruções deste tutorial, recomendamos que você se familiarize com o Terminologia e conceitos do Amazon Inspector Classic.

Este tutorial mostra como usar o Amazon Inspector Classic para analisar o comportamento de uma instância EC2 que executa o sistema operacional Ubuntu Server 16.04 LTS. Fornece instruções passo a passo sobre como navegar pelo fluxo de trabalho do Amazon Inspector Classic.

Se você for um usuário iniciante e quiser configurar e executar uma avaliação do Amazon Inspector Classic com um clique, consulte Criação de uma avaliação básica.

Tópicos

- Etapa 1: configurar uma instância do Amazon EC2 para usar com o Amazon Inspector Classic
- Etapa 2: criar um destino de avaliação e instalar um agente na instância EC2
- Etapa 3: criar e executar o modelo de avaliação
- Etapa 4: localizar e analisar as descobertas geradas

- Etapa 5: aplicar a correção recomendada ao destino de avaliação

Etapa 1: configurar uma instância do Amazon EC2 para usar com o Amazon Inspector Classic

Para configurar uma instância do EC2

- Para este tutorial, crie uma instância do EC2 executando o Ubuntu Server 16.04 LTS e marque-a usando a chave Nome e um valor de **`InspectorEC2InstanceUbuntu`**.

> **Note**
>
> Para mais informações sobre a marcação de instâncias do EC2, consulte Recursos e tags.

Etapa 2: criar um destino de avaliação e instalar um agente na instância EC2

O Amazon Inspector Classic usa destinos de avaliação para designar os recursos da AWS para avaliar.

Para criar um destino de avaliação e instalar um agente na instância EC2

1. Faça login no AWS Management Console e abra o console do Amazon Inspector Classic em https://console.aws.amazon.com/inspector/.
2. No painel de navegação, escolha Destinos de avaliação e, em seguida, Criar.
3. Em Nome, insira o nome do seu destino de avaliação.

   Para este tutorial, digite **`MyTargetUbuntu`**.
4. Para Usar tags, escolha as instâncias do EC2 que você quer incluir no destino de avaliação, inserindo valores para os campos Chave e Valor.

   Para este tutorial, escolha a instância do EC2 que você criou na etapa anterior, inserindo **`Name`** no campo Chave e **`InspectorEC2InstanceUbuntu`** no campo Valor.

Para incluir todas as instâncias do EC2 na conta da AWS e a região no destino de avaliação, selecione a caixa Todas as instâncias.

5. Instale um agente do Amazon Inspector Classic em sua instância do EC2 marcada. Para instalar um agente em todas as instâncias do EC2 incluídas em um destino de avaliação, selecione a caixa Instalar agentes.

   > **Note**
   >
   > Você também pode instalar o agente do Amazon Inspector usando o Executar Comando do Systems Manager. Para instalar o agente em todas instâncias na meta de avaliação, você pode especificar as mesmas tags usadas para a criação do destino de avaliação. Ou você pode instalar o agente do Amazon Inspector em sua instância do EC2 manualmente. Para obter mais informações, consulte Instalação de agentes do Amazon Inspector Classic.

6. Escolha Save (Salvar).

> **Note**
>
> Nesse ponto, uma função vinculada ao serviço `AWSServiceRoleForAmazonInspector` é criada para fornecer acesso do Amazon Inspector Classic aos seus recursos. Para obter mais informações, consulte Criação de um perfil vinculado a serviço para Amazon Inspector Classic.

Etapa 3: criar e executar o modelo de avaliação

Para criar e executar seu modelo

1. Se estiver usando Advanced Setup (Configuração avançada), você será direcionado para a página Define an assessment template (Definir um modelo de avaliação). Caso contrário, navegue até a página Assessment templates (Modelos de avaliação), e depois selecione Create (Criar).
2. Em Nome, insira o nome de seu modelo de avaliação. Para este tutorial, insira **`MyFirstTemplateUbuntu`**.
3. Em Nome do destino, escolha o destino de avaliação que você criou acima, **`MyTargetUbuntu`**.

4. Em Pacotes de regras, use o menu suspenso para selecionar os pacotes de regras que você deseja usar neste modelo de avaliação.

   Para este tutorial, escolha Vulnerabilidades e exposições comuns-1.1.

5. Em Duração, especifique a duração do modelo de avaliação.

   Para este tutorial, selecione 15 minutos.

6. Se estiver usando Configuração avançada, escolha Próximo. Na página Revisar a seguir, escolha Criar. Caso contrário, escolha Create and run (Criar e executar).

Etapa 4: localizar e analisar as descobertas geradas

Uma execução de avaliação concluída produz um conjunto de descobertas ou possíveis problemas de segurança que o Amazon Inspector Classic descobre no seu destino de avaliação. Você pode analisar as descobertas e seguir as etapas recomendadas para solucionar os possíveis problemas de segurança.

1. Navegue até a página Execuções de avaliação. Verifique se o status da execução do modelo de avaliação chamado MyFirstTemplateUbuntu que criou na etapa anterior está definido como Coleção de dados. Isso indica que a execução da avaliação está atualmente em andamento e os dados da telemetria para sua meta estão sendo coletados e analisados em relação aos pacotes de regras selecionados.
2. Não é possível visualizar as descobertas geradas pela execução da avaliação enquanto ela ainda estiver em andamento. Deixe a demonstração executar totalmente por toda a duração.

   O status de MyFirstTemplateUbuntu muda primeiro para Interrupção, para Análise depois de alguns minutos e, finalmente, Análise concluída. Para ver essas alterações no status, escolha o ícone Atualizar.

3. Navegue até a página Descobertas.

   Para expandir a exibição e ver os detalhes dessa descoberta, selecione a seta à esquerda da descoberta. Os detalhes da descoberta incluem o seguinte:

   - ARN da descoberta
   - Nome da execução da avaliação que produziu a descoberta
   - Nome do destino de avaliação que produziu a descoberta
   - Nome do modelo de avaliação que produziu a descoberta

- O horário de início da execução da avaliação
- O horário de término da execução da avaliação
- O status da execução da avaliação
- O nome do pacote de regras que inclui a regra que desencadeou a descoberta
- ID do agente do Amazon Inspector Classic
- O nome da descoberta
- A severidade da descoberta
- A descrição da descoberta
- Etapas de solução recomendadas que você pode concluir para corrigir o possível problema de segurança descrito pela descoberta

Etapa 5: aplicar a correção recomendada ao destino de avaliação

Neste procedimento, você aplica uma atualização para corrigir os problemas descobertos.

1. Conecte-se à sua instância **`InspectorEC2InstanceUbuntu`** e realize uma atualização do pacote.
2. Na página Modelos de avaliação, selecione MyFirstTemplateUbuntu e, em seguida, escolha Executar para iniciar uma nova execução de avaliação usando esse modelo.
3. Siga as etapas em Etapa 4: localizar e analisar as descobertas geradas para ver as descobertas que resultam dessa execução subsequente do modelo MyFirstTemplateUbuntu.

   A atualização do pacote deveria ter resolvido as descobertas da primeira execução do modelo.

Segurança no Amazon Inspector Classic

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

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

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam ao Amazon Inspector Classic consulte Serviços da AWS em Escopo por Programa de Conformidade
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação te ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Amazon Inspector Classic. Os tópicos a seguir mostram como configurar o Amazon Inspector Classic. para atender aos seus objetivos de segurança e conformidade. Saiba também como usar outros serviços da AWS que ajudam você a monitorar e proteger os recursos do Amazon Inspector Classic.

Tópicos

- Práticas recomendadas de segurança para o Amazon Inspector Classic

Proteção de dados no Amazon Inspector Classic

O modelo de responsabilidade AWS compartilhada se aplica à proteção de dados no Amazon Inspector Classic. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas Frequentes sobre Privacidade de Dados.. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Amazon Inspector Classic 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 de dados em repouso

Os dados de telemetria que um agente do Amazon Inspector Classic gera durante as execuções de avaliação são formatados em arquivos JSON. Esses arquivos são entregues via near-real-time TLS para o Amazon Inspector Classic, onde são criptografados com per-assessment-run uma chave derivada AWS KMS efêmera.

Os arquivos são armazenados com segurança em buckets do S3 dedicados do Amazon Inspector Classic. O mecanismo de regras do Amazon Inspector Classic faz o seguinte:

- Acessa os dados de telemetria criptografados no bucket do S3
- Descriptografa-os na memória
- Processa os dados em relação às regras de avaliação configuradas para gerar descobertas

Criptografia de dados em trânsito

Como um serviço gerenciado, o Amazon Inspector Classic 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 Classic pela rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

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

Identity and Access Management para Amazon Inspector Classic

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

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 Classic.

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 Classic 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 do Amazon Inspector Classic.

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 usuário do Usuário raiz da conta da AWS 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 Guia do Usuário do AWS IAM Identity Center . Usar a autenticação multifator (MFA) na AWS no Guia do Usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder 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 acessam 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 Manual do Usuário do AWS IAM Identity Center .

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 contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

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

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte Utilizar perfis 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 Criar um perfil para um provedor de identidades de terceiros no Guia do Usuário do IAM. Se você usar o Centro de identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM –- um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas –- é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM 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 do principal de chamada, usando um perfil de serviço ou um perfil vinculado a 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: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM, consulte Quando criar um perfil 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 permissões 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 presumir os perfis.

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. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do Usuário do IAM.

Políticas baseadas em recursos

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

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas 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 perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo 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 com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do Usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte Como os SCPs Funcionam no Manual do Usuário do AWS Organizations .
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do Usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como o Amazon Inspector Classic 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 Classic

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
Funções vinculadas ao serviço	Sim

Para obter uma visão de alto nível de como o Amazon Inspector e AWS outros serviços funcionam com a maioria dos recursos do IAM, AWS consulte os serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade do Amazon Inspector

Suporta políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte 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 perfil ao 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 do Amazon Inspector Classic.

Políticas baseadas em recursos no Amazon Inspector

Oferece compatibilidade com 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 perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado

pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

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 recurso 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 recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações de políticas para o Amazon Inspector

Oferece compatibilidade com 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. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

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:

```
inspector
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
      "inspector:action1",
      "inspector:action2"
         ]
```

A política de permissões a seguir concede permissão a um usuário para executar todas as operações que começam com `Describe` e `List`. Essas operações mostram informações sobre um recurso do Amazon Inspector, como uma descoberta ou um destino de avaliação. O caractere curinga (*) no elemento `Resource` indica que as operações são permitidas para todos os recursos do Amazon Inspector que pertencem à conta:

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

Exemplo 2: Permitir que um usuário execute, descreva e liste apenas em descobertas do Amazon Inspector

A política de permissões a seguir concede permissão para um usuário executar apenas operações `ListFindings` e `DescribeFindings`. Essas operações mostram informações sobre descobertas do Amazon Inspector. O caractere curinga (*) no elemento `Resource` indica que as operações são permitidas para todos os recursos do Amazon Inspector que pertencem à conta.

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

```
      {
         "Effect":"Allow",
         "Action": [
                  "inspector:DescribeFindings",
                  "inspector:ListFindings"
         ],
         "Resource":"*"
      }
   ]
}
```

Para ver exemplos de políticas baseadas em identidade do Amazon Inspector, consulte Exemplos de políticas baseadas em identidade do Amazon Inspector Classic.

Recursos de política do Amazon Inspector

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

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

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

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 Classic.

Para ver exemplos de políticas baseadas em identidade do Amazon Inspector, consulte Exemplos de políticas baseadas em identidade do Amazon Inspector Classic.

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 entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

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

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, 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 da 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 Classic.

Para ver exemplos de políticas baseadas em identidade do Amazon Inspector, consulte Exemplos de políticas baseadas em identidade do Amazon Inspector Classic.

ACLs no Amazon Inspector

Oferece compatibilidade com ACLs	Não

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

ABAC com o Amazon Inspector

Oferece compatibilidade com 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 onde o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou chaves de condição `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso por atributo (ABAC) no Guia do usuário do IAM.

Usar credenciais temporárias com o Amazon Inspector

Oferece compatibilidade com 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 um perfil (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte Credenciais de segurança temporárias no IAM.

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 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

Um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **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 presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas a serviço do Amazon Inspector, consulte Uso de funções vinculadas a serviço para o Amazon Inspector Classic.

Exemplos de políticas baseadas em identidade do Amazon Inspector Classic

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 aos usuários permissão para executar

ações nos recursos de que precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir 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 Classic 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 que um usuário execute operações de descrição e listagem apenas em descobertas 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 as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS 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.

- Use condições nas políticas do IAM para restringir ainda mais o acesso –- você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode 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 Elementos da política JSON do IAM: Condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais –- o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para 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 Classic, 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 que um usuário execute operações de descrição e listagem apenas em descobertas do Amazon Inspector

A política de permissões a seguir concede permissão para um usuário executar apenas operações `ListFindings` e `DescribeFindings`. Essas operações mostram informações sobre descobertas do Amazon Inspector. O caractere curinga (*) no elemento `Resource` indica que as operações são permitidas para todos os recursos do Amazon Inspector que pertencem à conta.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                  "inspector:DescribeFindings",
                  "inspector:ListFindings"
         ],
         "Resource":"*"
      }
   ]
}
```

Uso de funções vinculadas a serviço para o Amazon Inspector Classic

O Amazon Inspector Classic usa funções vinculadas a serviços AWS Identity and Access Management (IAM). Perfil vinculado a serviço é um tipo especial de perfil do IAM que é vinculado diretamente ao Amazon Inspector Classic. Os perfis vinculados a serviço são definidos previamente pelo Amazon Inspector Classic. e incluem todas as permissões que o serviço requer para chamar outros serviços da Serviços da AWS em seu nome.

O perfil vinculado a serviço facilita a configuração do Amazon Inspector Classic porque você não precisa adicionar as permissões necessárias manualmente. O Amazon Inspector Classic define as permissões dos perfis vinculados a serviço e, exceto se definido de outra forma, somente o Amazon Inspector Classic pode assumir suas funções. As permissões definidas incluem as políticas de confiança e de permissões, e essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Você só pode excluir um perfil vinculado a serviço depois de excluir os recursos relacionados. Isso protege seus recursos do Amazon Inspector Classic, pois você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com perfis vinculados aos serviços, consulte Serviços da AWS que funcionam com o IAM e procure os serviços que apresentam Sim na coluna Funções vinculadas aos serviços. Escolha um Sim com um link para ver a documentação do perfil vinculado a esse serviço.

Permissões de perfil vinculado a serviço para o Amazon Inspector Classic.

O Amazon Inspector Classic usa a função vinculada ao serviço chamada —. AWSServiceRoleForAmazonInspector ServiceLinkedRoleDescription

A função AWSServiceRoleForAmazonInspector vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `inspector.amazonaws.com`

A política de permissões de função nomeada AmazonInspectorServiceRolePolicy permite que o Amazon Inspector Classic conclua as seguintes ações nos recursos especificados:

- Ação: `iam:CreateServiceLinkedRole` em `arn:aws:iam::*:role/aws-service-role/inspector.amazonaws.com/AWSServiceRoleForAmazonInspector`

É necessário configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou perfil) crie, edite ou exclua um perfil vinculado a serviço. Para ter mais informações, consulte Service-linked role permissions (Permissões de nível vinculado a serviços) no Guia do usuário do IAM.

Criação de um perfil vinculado a serviço para Amazon Inspector Classic

Não é necessário criar manualmente um perfil vinculado a serviço. Quando você está CompleteThisCreateActionInThisService na AWS Management Console, na ou na AWS API AWS CLI, o Amazon Inspector Classic cria a função vinculada ao serviço para você.

Editar um perfil vinculado a serviço do Amazon Inspector Classic

O Amazon Inspector Classic não permite que você edite a função vinculada ao AWSServiceRoleForAmazonInspector serviço. Depois que criar um perfil vinculado ao serviço, você

não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para ter mais informações, consulte Editar um perfil vinculado a serviço no Guia do usuário do IAM.

Excluir um perfil vinculado a serviço do Amazon Inspector Classic

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado a serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ou mantida ativamente. No entanto, você deve limpar os recursos do seu perfil vinculado a serviço antes de exclui-lo manualmente.

> **Note**
>
> Se o serviço do Amazon Inspector Classic estiver usando o perfil quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir recursos do Amazon Inspector Classic usados por **`AWSServiceRoleForAmazonInspector`**

- Exclua suas metas de avaliação para isso Conta da AWS em todos os Regiões da AWS lugares em que você tem o Amazon Inspector Classic em execução. Para ter mais informações, consulte Destinos de avaliação do Amazon Inspector Classic.

Como excluir manualmente o perfil vinculado a serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSServiceRoleForAmazonInspector vinculada ao serviço. Para obter mais informações, consulte Excluir um perfil vinculado a serviço no Guia do usuário do IAM.

Regiões com suporte para perfis vinculados a serviço do Amazon Inspector Classic

O Amazon Inspector Classic oferece suporte usando funções vinculadas a serviços em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte Regiões e endpoints da AWS.

Solução de problemas de identidade e acesso do Amazon Inspector Classic

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

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 `inspector:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 inspector: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 `inspector:`*`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 um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

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

Registro em log e monitoramento no Amazon Inspector Classic

O Amazon Inspector Classic está integrado com AWS CloudTrail, um serviço que fornece um registro das ações tomadas por um usuário, função ou AWS serviço no Amazon Inspector Classic. CloudTrail captura todas as chamadas de API para o Amazon Inspector Classic como eventos, incluindo chamadas do console do Amazon Inspector Classic e chamadas de código para as operações de API do Amazon Inspector Classic.

Para obter informações sobre como usar o CloudTrail registro no Amazon Inspector Classic, consulte. Log de chamadas de API da Amazon Inspector Classic com o AWS CloudTrail

Você pode monitorar o Amazon Inspector Classic usando a Amazon CloudWatch, que coleta e processa dados brutos em métricas legíveis e quase em tempo real. Por padrão, o Amazon Inspector Classic envia dados métricos CloudWatch em períodos de 5 minutos.

Para obter informações sobre como usar CloudWatch com o Amazon Inspector Classic, consulte. Monitorar o Amazon Inspector Classic usando o Amazon CloudWatch

Resposta a incidentes no Amazon Inspector Classic

A resposta a incidentes do Amazon Inspector Classic é uma AWS responsabilidade. AWS tem uma política e um programa formais e documentados que regem a resposta a incidentes.

AWS problemas operacionais com amplo impacto são publicados no AWS Service Health Dashboard.

As emissões operacionais também são publicadas em contas individuais por meio do AWS Health Dashboard. Para obter informações sobre como usar o AWS Health Dashboard, consulte o Guia AWS Health do usuário.

Validação de conformidade do Amazon Inspector Classic

Auditores terceirizados avaliam a segurança e a conformidade do Amazon Inspector Classic como parte de AWS vários programas de conformidade. Isso inclui SOC, PCI, FedRAMP, HIPAA e outros.

Para obter uma lista de AWS serviços no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo do programa de conformidade . Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Fazer download de relatórios no AWS Artifact.

Sua responsabilidade de conformidade ao usar o Amazon Inspector Classic é determinada pela sensibilidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelas leis e regulamentos aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido de segurança e compatibilidade: estes guias de implantação abordam as considerações de arquitetura e fornecem etapas para implantação de ambientes de linha de base focados em compatibilidade e segurança na AWS.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos compatíveis com a 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.
- 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— Esse AWS serviço fornece uma visão abrangente do seu estado de segurança interno, AWS que ajuda você a verificar sua conformidade com os padrões e as melhores práticas do setor de segurança.

Resiliência no Amazon Inspector Classic

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicativos e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

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

O Amazon Inspector Classic é altamente disponível e executa consultas usando recursos de computação em várias zonas de disponibilidade. Ele roteia de forma automática as consultas adequadamente se determinada zona de disponibilidade estiver inacessível.

O Amazon Inspector Classic usa o Amazon S3 como seu banco de dados subjacente, o que torna os dados altamente disponíveis e duráveis. O Amazon S3 dispõe de uma infraestrutura durável para armazenar dados importantes. Ele é criado para uma durabilidade de objetos de 99,999999999% Seus dados são armazenados com redundância em várias instalações e diversos dispositivos em cada instalação.

Segurança da infraestrutura no Amazon Inspector Classic

Como um serviço gerenciado, o Amazon Inspector Classic 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 Classic pela rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

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

Para obter mais informações sobre segurança de rede e agente do Amazon Inspector Classic, consulte the section called “Segurança da rede e do agente do Amazon Inspector Classic”.

Análise de configuração e vulnerabilidade no Amazon Inspector Classic

O Amazon Inspector Classic oferece software predefinido chamado de agente que você pode instalar no sistema operacional das instâncias do EC2 que você quer avaliar. O agente coleta um amplo conjunto de dados de configuração, conhecido como telemetria. Para mais informações sobre os agentes do Amazon Inspector Classic, consulte Agentes do Amazon Inspector Classic.

Práticas recomendadas de segurança para o Amazon Inspector Classic

O Amazon Inspector Classic fornece uma série de recursos de segurança a serem considerados no desenvolvimento e na implementação das suas próprias políticas de segurança. Essas melhores práticas são diretrizes gerais e não representam uma solução completa de segurança. Como essas melhores práticas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como considerações úteis em vez de prescrições.

Para obter a lista de práticas de segurança recomendadas para o Amazon Inspector Classic, consulte the section called “Práticas recomendadas de segurança para o Amazon Inspector Classic”.

Agentes do Amazon Inspector Classic

O agente do Amazon Inspector Classic é uma entidade que coleta informações de pacotes instalados e a configuração de software para uma instância do Amazon EC2. Embora não seja necessário em todos os casos, você deve instalar o agente do Amazon Inspector Classic em cada uma das instâncias da meta do Amazon EC2 para avaliar totalmente sua segurança.

Para obter mais informações sobre como instalar, desinstalar e reinstalar o agente, como verificar se o agente instalado está em execução e como configurar o suporte de proxy do agente, consulte Trabalhar com agentes do Amazon Inspector Classic em sistemas operacionais baseados em Linux e Trabalhar com agentes do Amazon Inspector Classic em sistemas operacionais baseados em Windows.

> **Note**
>
> Um agente do Amazon Inspector Classic não é necessário para executar o pacote de regras da Acessibilidade de rede.

> **Important**
>
> O agente do Amazon Inspector Classic depende dos metadados da instância do Amazon EC2 para funcionar corretamente. Ele acessa os metadados da instância usando a versão 1 ou a versão 2 do Serviço de Metadados da Instância (IMDSv1 ou IMDSv2). Consulte Metadados da instância e dados do usuário para saber mais sobre os metadados da instância do EC2 e os métodos de acesso.

Tópicos

- Instalação de agentes do Amazon Inspector Classic
- Trabalhar com agentes do Amazon Inspector Classic em sistemas operacionais baseados em Linux
- Trabalhar com agentes do Amazon Inspector Classic em sistemas operacionais baseados em Windows
- (Opcional) Verifique a assinatura do script de instalação do agente do Amazon Inspector Classic em sistemas operacionais baseados em Linux
- (Opcional) Verifique a assinatura do script de instalação do agente do Amazon Inspector Classic em sistemas operacionais baseados em Windows

Privilégios do agente do Amazon Inspector Classic

Você deve ter permissões administrativas ou de raiz para instalar o agente do Amazon Inspector Classic. Em sistemas operacionais baseados em Linux compatíveis, o agente consiste em um executável de modo de usuário que é executado com acesso raiz. Em sistemas operacionais compatíveis baseados em Windows, o agente consiste em um serviço atualizador e um serviço de agente, cada um em execução no modo de usuário com privilégios `LocalSystem`.

Segurança da rede e do agente do Amazon Inspector Classic

O agente do Amazon Inspector Classic inicia toda a comunicação com o serviço Amazon Inspector Classic. Isso significa que o agente deve ter um caminho de rede de saída para endpoints públicos, para que possa enviar dados de telemetria. Por exemplo, o agente pode se conectar a `arsenal.<region>.amazonaws.com` e o endpoint pode ser um bucket do Amazon S3 na `s3.dualstack.<region>.amazonaws.com`. Certifique-se de `<region>` substituir pela AWS região real em que você está executando o Amazon Inspector Classic. Para obter mais informações, consulte Intervalos de endereço IP da AWS. Como todas as conexões do agente são chamadas de saída estabelecidas, não é necessário abrir portas em seus grupos de segurança para permitir comunicações de entrada para o agente do Amazon Inspector Classic.

O agente se comunica periodicamente com o Amazon Inspector Classic por meio de um canal protegido por TLS, que é autenticado usando AWS a identidade associada à função da instância EC2 ou, se nenhuma função for atribuída, com o documento de metadados da instância. Uma vez autenticado, o agente envia mensagens de pulsação para o serviço e recebe instruções do serviço como resposta. Se uma avaliação tiver sido programada, o agente receberá as instruções para essa avaliação. Essas instruções são arquivos JSON estruturados, e informam o agente para habilitar ou

desabilitar sensores específicos pré-configurados no agente. Cada ação da instrução é predefinida no agente. Instruções arbitrárias não podem ser executadas.

Durante uma avaliação, o agente reúne os dados de telemetria do sistema para enviá-los de volta ao Amazon Inspector Classic por meio de um canal protegido por TLS. O agente não faz alterações no sistema do qual ele coleta dados. Após coletar dados de telemetria, o agente envia os dados de volta ao Amazon Inspector Classic para processamento. Além dos dados de telemetria que ele gera, o agente não é capaz de coletar ou transmitir qualquer outro dado sobre o sistema ou os destinos de avaliação. No momento, não há nenhum método exposto para interceptar e examinar os dados de telemetria no agente.

Atualizações do agente do Amazon Inspector Classic

À medida que as atualizações do agente do Amazon Inspector Classic são disponibilizadas, elas são automaticamente obtidas por download do Amazon S3 e aplicadas. Isso também atualiza qualquer dependência necessária. O recurso de atualização automática elimina a necessidade de rastrear e manter manualmente o controle de versões dos agentes que você instalou em suas instâncias do EC2. Todas as atualizações estão sujeitas aos processos auditados de controle de alterações da Amazon para garantir a conformidade com as normas de segurança aplicáveis.

Para garantir ainda mais a segurança do agente, todas as comunicações entre o agente e o site de liberação de atualizações automáticas (S3) são realizadas por meio de uma conexão TLS e o servidor é autenticado. Todos os binários envolvidos no processo de atualização automática são assinados digitalmente e as assinaturas são verificadas pelo atualizador antes da instalação. O processo de atualização automática é executado somente durante os períodos sem avaliação. Se algum erro for detectado, o processo de atualização poderá ser revertido e tentará fazer a atualização novamente. Por fim, o processo de atualização do agente serve para atualizar somente os recursos do agente. Nenhuma de suas informações específicas é enviada do agente para o Amazon Inspector Classic como parte do fluxo de trabalho de atualização. A única informação comunicada como parte do processo de atualização é a telemetria básica de sucesso ou falha da instalação e, se aplicável, informações de diagnóstico de falha da atualização.

Ciclo de vida dos dados de telemetria

Os dados de telemetria que são gerados pelo agente do Amazon Inspector Classic durante execuções de avaliação são formatados em arquivos JSON. Os arquivos são entregues via TLS para near-real-time o Amazon Inspector Classic, onde são criptografados com per-assessment-run uma

chave efêmera derivada do KMS. Os arquivos são armazenados com segurança em um bucket do Amazon S3 dedicado ao Amazon Inspector Classic. O mecanismo de regras do Amazon Inspector Classic acessa os dados de telemetria criptografados no bucket do S3, descriptografa os dados na memória e os processa com base nas regras de avaliação configuradas para gerar descobertas. Os dados de telemetria que são armazenados no S3 são retidos somente para permitir a assistência a solicitações de suporte. Eles não são usados ou agregados pela Amazon para qualquer outra finalidade. Após 30 dias, os dados de telemetria são excluídos permanentemente de acordo com a política de ciclo de vida padrão de um bucket do S3 para dados do Amazon Inspector Classic. No momento, o Amazon Inspector Classic não fornece uma API ou um mecanismo de acesso ao bucket do S3 para a telemetria coletada.

Controle de acesso do Amazon Inspector Classic em contas AWS

Como um serviço de segurança, o Amazon Inspector Classic acessa suas AWS contas e recursos somente quando precisa encontrar instâncias do EC2 para avaliar, consultando tags. Isso é feito por meio do acesso padrão do IAM pela função criada durante a configuração inicial do serviço Amazon Inspector Classic. Durante uma avaliação, todas as comunicações com seu ambiente são iniciadas pelo agente do Amazon Inspector Classic que está instalado localmente nas instâncias do EC2. Os objetos do serviço Amazon Inspector Classic que são criados, como os destinos de avaliação, os modelos de avaliação e as descobertas geradas pelo serviço, são armazenados em um banco de dados gerenciado pelo Amazon Inspector Classic e acessível somente por ele.

Limites do agente do Amazon Inspector Classic

Para obter mais informações sobre os limites do agente do Amazon Inspector Classic, consulte Limites do serviço do Amazon Inspector Classic.

Instalação de agentes do Amazon Inspector Classic

Você pode instalar o agente do Amazon Inspector Classic usando o Run Command do Systems Manager em várias instâncias (incluindo instâncias baseadas em Linux e Windows). Como alternativa, você pode instalar o agente individualmente, conectando-se a cada instância EC2 . Os procedimentos neste capítulo fornecem instruções para ambos os métodos.

Como outra opção, você pode instalar rapidamente o agente em todas as instâncias do Amazon EC2 incluídas em um destino de avaliação selecionando a opçãoInstalar agentes na página Definir um destino de avaliação) no console.

Tópicos

> **Note**
>
> Os procedimentos deste capítulo se aplicam a todas as AWS regiões que são suportadas pelo Amazon Inspector Classic.

Como instalar o agente em várias instâncias do EC2 usando o Executar Comando do Systems Manager

Você pode instalar o agente do Amazon Inspector Classic em suas instâncias do EC2 usando o Executar Comando do Systems Manager. Isso possibilita instalar o agente remotamente em várias instâncias (instâncias baseadas em Linux e em Windows com o mesmo comando) de uma só vez.

> **Important**
>
> A instalação do agente usando o Executar Comando do Systems Manager atualmente não é compatível com o sistema operacional Debian.

> **Important**
>
> Para utilizar essa opção, certifique-se de que sua instância do EC2 tem o Agente SSM instalado e tem uma função do IAM que permite o Executar Comando. O Agente SSM é instalado, por padrão, em instâncias do Windows no Amazon EC2 e do Amazon Linux. O Amazon EC2 Systems Manager requer uma função do IAM para instâncias do EC2 que processa comandos e uma função separada para usuários que executam comandos. Para mais informações, consulte Como instalar e configurar o Agente SSM e Como configurar funções de segurança para o System Manager.

Para instalar o agente em várias instâncias do EC2 usando o comando de execução Systems Manager

1. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.
2. No painel de navegação, em Instâncias e nós, selecione Executar comando.
3. Escolha Executar um comando.
4. Em Documento de comando, escolha o documento chamado AmazonInspector-Manage AWSAgent que é de propriedade da Amazon. Esse documento contém o script de instalação do agente do Amazon Inspector Classic em instâncias do EC2.
5. Em Destinos, você pode escolher instâncias EC2 usando métodos diferentes. Para instalar o agente em todas as instâncias no destino de avaliação, é possível especificar as tags que foram usada para criar o destino de avaliação.
6. Forneça suas opções para as demais opções disponíveis usando as instruções em Executar comandos do console e selecione Run (Executar).

> **Note**
>
> Você também pode instalar o agente em várias instâncias EC2 (baseadas em Linux e Windows) ao criar um destino de avaliação, ou você pode usar o botão Instalar agentes com o comando Run para um destino existente. Para ter mais informações, consulte Como criar um destino de avaliação.

Como instalar o agente em uma instância do EC2 baseada em Linux

Execute o procedimento a seguir para instalar o agente do Amazon Inspector Classic em uma instância EC2 baseada em Linux.

Para instalar o agente em uma instância do EC2 baseada em Linux

1. Conecte-se à sua instância do EC2, que está executando um sistema operacional baseado em Linux, da qual você deseja desinstalar o agente do Amazon Inspector Classic.

> **Note**
>
> Para obter informações sobre os sistemas operacionais compatíveis com o Amazon Inspector Classic, consulte Sistemas operacionais e regiões compatíveis com o Amazon Inspector Classic.

2. Baixe o script de instalação do agente executando um dos comandos a seguir:

   - wget https://inspector-agent.amazonaws.com/linux/latest/install
   - curl -O https://inspector-agent.amazonaws.com/linux/latest/install

3. (Opcional) Verifique se o script de instalação do agente não foi alterado ou corrompido. Para ter mais informações, consulte (Opcional) Verifique a assinatura do script de instalação do agente do Amazon Inspector Classic em sistemas operacionais baseados em Linux.

4. Para instalar o agente, execute sudo bash install.

> **Note**
>
> Se você estiver instalando o agente em um ambiente SELinux, o Amazon Inspector Classic pode ser detectado como um daemon não confinado. Você pode evitar isso alterando o domínio do processo do agente do padrão `initrc_t` para `bin_t`. Use os seguintes comandos para atribuir o `bin_t` contexto aos scripts de execução do Amazon Inspector Classic antes de instalar o agente para o SELinux:
> sudo semanage fcontext -a -t bin_t /etc/rc\.d/init\.d/awsagent
> sudo semanage fcontext -a -t bin_t /etc/init\.d/awsagent

> **Note**
>
> À medida que as atualizações do agente são disponibilizadas, elas são automaticamente baixadas do Amazon S3 e aplicadas. Para ter mais informações, consulte Atualizações do agente do Amazon Inspector Classic.
> Se você deseja ignorar esse processo de atualização automática, execute este comando ao instalar o agente:
> sudo bash install -u false

> **Note**
>
> (Opcional) Para remover o script de instalação do agente, execute rm install.

5. Verifique se os seguintes arquivos necessários para o agente ser instalado com êxito e funcionar corretamente estão instalados:

   - `libcurl4` (necessário para instalar o agente no Ubuntu 18.04)
   - `libcurl3`
   - `libgcc1`
   - `libc6`
   - `libstdc++6`
   - `libssl1.0.1`
   - `libssl1.0.2` (necessário para instalar o agente no Debian 9)
   - `libssl1.1` (necessário para instalar o agente no Ubuntu 20.04 LTS)
   - `libpcap0.8`

Como instalar o agente em uma instância do EC2 baseada em Windows

Execute o procedimento a seguir para instalar o agente do Amazon Inspector Classic em uma instância EC2 baseada em Windows.

Para instalar o agente em uma instância do EC2 baseada em Windows

1. Conecte-se à sua instância do EC2 executando um sistema operacional baseado em Windows em que você deseja instalar o agente.

   > **Note**
   >
   > Para obter mais informações sobre os sistemas operacionais compatíveis com o Amazon Inspector Classic, consulte Sistemas operacionais e regiões compatíveis com o Amazon Inspector Classic.

2. Faça download do seguinte arquivo .exe:

```
https://inspector-agent.amazonaws.com/windows/installer/latest/
AWSAgentInstall.exe
```

3. Abra uma janela de prompt de comando (com permissões administrativas), navegue até o local onde você salvou o `AWSAgentInstall.exe` obtido por download e execute o arquivo .exe para instalar o agente.

> **Note**
>
> À medida que as atualizações do agente são disponibilizadas, elas são automaticamente baixadas do Amazon S3 e aplicadas. Para ter mais informações, consulte Atualizações do agente do Amazon Inspector Classic.
> Se você deseja ignorar esse processo de atualização automática, execute este comando ao instalar o agente:
> AWSAgentInstall.exe AUTOUPDATE=No

Trabalhar com agentes do Amazon Inspector Classic em sistemas operacionais baseados em Linux

É possível instalar, remover, verificar e modificar o comportamento dos agentes do Amazon Inspector Classic. Conecte-se à sua instância do Amazon EC2 com um sistema operacional Linux e execute um dos seguintes procedimentos. Para obter mais informações sobre os sistemas operacionais compatíveis com o Amazon Inspector Classic, consulte Sistemas operacionais e regiões compatíveis com o Amazon Inspector Classic.

> **Important**
>
> O agente do Amazon Inspector Classic depende dos metadados da instância do Amazon EC2 para funcionar corretamente. Ele acessa os metadados da instância usando a versão 1 ou a versão 2 do Serviço de Metadados da Instância (IMDSv1 ou IMDSv2). Consulte Metadados da instância e dados do usuário para saber mais sobre os metadados da instância do EC2 e os métodos de acesso.

> **Note**
>
> Os comandos nesta seção funcionam em todas as AWS regiões que são suportadas pelo Amazon Inspector Classic.

Tópicos

Verificar se o agente do Amazon Inspector Classic está em execução

- Para verificar se o agente está instalado e em execução, faça login em sua instância do EC2 e execute o seguinte comando:

  sudo /opt/aws/awsagent/bin/awsagent status

  Esse comando retornará o status do agente em execução no momento ou um erro indicando que o agente não pode ser contatado.

Interromper o agente do Amazon Inspector Classic

- Para interromper o agente, execute o seguinte comando:

  sudo /etc/init.d/awsagent stop

Iniciar o agente do Amazon Inspector Classic

- Para iniciar o agente, execute o seguinte comando:

  sudo /etc/init.d/awsagent start

Modificar as configurações do agente do Amazon Inspector Classic

Assim que o agente do Amazon Inspector Classic estiver instalado e em execução na sua instância do EC2, você poderá modificar as configurações no arquivo `agent.cfg` para alterar o comportamento do agente. Em sistemas operacionais Linux, o arquivo `agent.cfg` está localizado no diretório `/opt/aws/awsagent/etc`. Depois de modificar e salvar o arquivo `agent.cfg`, você deverá interromper e iniciar o agente para que as alterações sejam aplicadas.

> **Important**
>
> É altamente recomendável que você só modifique o arquivo `agent.cfg` com a orientação do AWS Support.

Configurar o suporte de proxy para um agente do Amazon Inspector Classic

Para obter suporte de proxy para um agente em um sistema operacional Linux, use um arquivo de configuração específico do agente com variáveis de ambiente específicas. Para obter mais informações, consulte https://wiki.archlinux.org/index.php/proxy_settings.

Conclua um dos seguintes procedimentos:

Para instalar um agente em uma instância do EC2 que usa um servidor de proxy

1. Crie um arquivo chamado `awsagent.env` e salve-o no diretório `/etc/init.d/`.
2. Edite `awsagent.env` para incluir essas variáveis de ambiente no seguinte formato:

   - `export https_proxy=hostname:port`
   - `export http_proxy=hostname:port`
   - `export no_proxy=169.254.169.254`

> **Note**
>
> Substitua os valores dos exemplos acima somente por combinações válidas do nome do host e do número da porta. Especifique o endereço IP do endpoint dos metadados da instância (169.254.169.254) para a variável `no_proxy`.

3. Instale o agente do Amazon Inspector Classic concluindo as etapas no procedimento Como instalar o agente em uma instância do EC2 baseada em Linux.

Para configurar o suporte de proxy em uma instância do EC2 com um agente em execução

1. Para configurar o suporte de proxy, a versão do agente que está em execução na sua instância do EC2 deve ser a 1.0.800.1 ou posterior. Se você habilitar o processo de atualização automática para o agente, será possível verificar se a versão do seu agente é 1.0.800.1 ou posterior usando o procedimento Verificar se o agente do Amazon Inspector Classic está em execução. Se você não habilitar o processo de atualização automática para o agente, deverá instalar o agente nesta instância do EC2 novamente seguindo o procedimento Como instalar o agente em uma instância do EC2 baseada em Linux.
2. Crie um arquivo chamado `awsagent.env` e salve-o no diretório `/etc/init.d/`.
3. Edite `awsagent.env` para incluir essas variáveis de ambiente no seguinte formato:

   - `export https_proxy=hostname:port`
   - `export http_proxy=hostname:port`
   - `export no_proxy=169.254.169.254`

   > **Note**
   >
   > Substitua os valores dos exemplos acima somente por combinações válidas do nome do host e do número da porta. Especifique o endereço IP do endpoint dos metadados da instância (169.254.169.254) para a variável `no_proxy`.

4. Reinicie o agente primeiramente interrompendo-o, usando o seguinte comando:

   ```
   sudo /etc/init.d/awsagent restart
   ```

   As configurações de proxy são selecionadas e usadas pelo agente e pelo processo de atualização automática.

Para desinstalar o agente do Amazon Inspector Classic

Para desinstalar o agente

1. Conecte-se à sua instância do EC2 executando o sistema operacional baseado em Linux onde você deseja desinstalar o agente da AWS.

   > **Note**
   >
   > Para obter mais informações sobre os sistemas operacionais compatíveis com o Amazon Inspector Classic, consulte Sistemas operacionais e regiões compatíveis com o Amazon Inspector Classic.

2. Para desinstalar o agente, use um dos seguintes comandos:

   - No Amazon Linux, CentOS e Red Hat, execute o seguinte comando:

     sudo yum remove 'AwsAgent*'

   - No Ubuntu Server, execute o seguinte comando:

     sudo apt-get purge 'awsagent*'

Trabalhar com agentes do Amazon Inspector Classic em sistemas operacionais baseados em Windows

É possível iniciar, interromper e modificar o comportamento dos agentes do Amazon Inspector Classic. Faça login em sua instância do EC2 usando um sistema operacional Windows e execute qualquer um dos seguintes procedimentos neste capítulo. Para obter mais informações sobre os sistemas operacionais compatíveis com o Amazon Inspector Classic, consulte Sistemas operacionais e regiões compatíveis com o Amazon Inspector Classic.

> **Important**
>
> O agente do Amazon Inspector Classic depende dos metadados da instância do Amazon EC2 para funcionar corretamente. Ele acessa os metadados da instância usando a versão 1 ou a versão 2 do serviço de metadados da instância - Instance Metadata Service - (IMDSv1

ou IMDSv2). Consulte Metadados da instância e dados do usuário para saber mais sobre os metadados da instância do EC2 e os métodos de acesso.

> **Note**
>
> Os comandos neste capítulo funcionam em todas as AWS regiões compatíveis com o Amazon Inspector Classic.

Tópicos

Como iniciar ou interromper um agente do Amazon Inspector Classic ou verificar se o agente está em execução

Para iniciar, interromper ou verificar um agente

1. Em sua instância do EC2 selecione (Iniciar, Executar e insira **`services.msc`**.
2. Se o agente estiver sendo executado com sucesso, dois serviços serão listados com os status definidos como Iniciado ou Em execução na janela Serviços: Serviço de agente da AWS e Serviço do atualizador de agente da AWS.
3. Para iniciar o agente, clique com o botão direito do mouse em Serviço de agente da AWS e selecione Iniciar. Se o serviço for iniciado com sucesso, o status será atualizado para Iniciado ou Em execução.
4. Para interromper o agente, clique com o botão direito do mouse em Serviço de agente da AWS e selecione Interromper. Se o serviço for interrompido com sucesso, o status será limpo (aparecerá em branco). Não recomendamos interromper o Serviço do atualizador de agente da AWS já que ele desativa a instalação de todos os futuros aprimoramentos e correções do agente.

5. Para verificar se o agente está instalado e em execução, faça login em sua instância do EC2 e abra um prompt de comando usando permissões administrativas. Navegue até `C:\Program Files\Amazon Web Services\AWS Agent` e execute o seguinte comando:

   AWSAgentStatus.exe

   Esse comando retornará o status do agente em execução no momento, ou um erro indicando que o agente não pode ser contatado.

Modificando as configurações do agente do Amazon Inspector Classic

Assim que o agente do Amazon Inspector Classic estiver instalado e em execução na sua instância do EC2, você poderá modificar as configurações no arquivo `agent.cfg` para alterar o comportamento do agente. Em sistemas operacionais Windows, o arquivo está localizado no diretório `C:\ProgramData\Amazon Web Services\AWS Agent`. Depois de modificar e salvar o arquivo `agent.cfg`, você deverá interromper e iniciar o agente para que as alterações sejam aplicadas.

> **Important**
>
> É altamente recomendável que você só modifique o arquivo `agent.cfg` com a orientação do AWS Support.

Configurar o suporte de proxy para um agente do Amazon Inspector Classic

Para obter suporte de proxy para um agente em um sistema operacional Windows, use o proxy `WinHTTP`. Para configurar o proxy `WinHTTP` usando o utilitário `netsh`, consulte Comandos Netsh para Windows Hypertext Transfer Protocol (WINHTTP).

> **Important**
>
> Somente proxies HTTPS são compatíveis com instâncias baseadas no Windows.

Conclua um dos seguintes procedimentos:

Para instalar um agente em uma instância do EC2 que usa um servidor de proxy

1. Baixe o arquivo .exe a seguir: `https://d1wk0tztpsntt1.cloudfront.net/windows/installer/latest/AWSAgentInstall.exe`
2. Abra uma janela de prompt de comando ou a janela do PowerShell (usando permissões administrativas). Navegue até o local onde você salvou o `AWSAgentInstall.exe` obtido por download e execute o seguinte comando:

   ```
   .\AWSAgentInstall.exe /install USEPROXY=1
   ```

Para configurar o suporte de proxy em uma instância do EC2 com um agente em execução

1. Para configurar o suporte de proxy, a versão do agente do Amazon Inspector Classic que está em execução em sua instância do EC2 deve ser a 1.0.0.59 ou posterior. Se você habilitar o processo de atualização automática para o agente, é possível verificar se a versão do seu agente é 1.0.0.59 ou posterior usando o procedimento Como iniciar ou interromper um agente do Amazon Inspector Classic ou verificar se o agente está em execução. Se você não habilitar o processo de atualização automática para o agente, deverá instalar o agente nesta instância do EC2 novamente seguindo o procedimento Como instalar o agente em uma instância do EC2 baseada em Windows.
2. Abra o editor de registros (`regedit.exe`).
3. Navegue até a seguinte chave de registro: `"HKEY_LOCAL_MACHINE/SOFTWARE/Amazon Web Services/AWS Agent Updater"`.
4. Dentro dessa chave de registro, crie um valor de registro `DWORD(32bit)` chamado `"UseProxy"`.
5. Clique duas vezes no valor e defina-o como 1.
6. Insira **`services.msc`**, localize o Serviço de agente da AWS e o Serviço do atualizador de agente da AWS na janela Serviços e reinicie cada processo. Após ambos os processos terem sido reiniciados com sucesso, execute o arquivo `AWSAgentStatus.exe` (consulte a etapa 5 em Como iniciar ou interromper um agente do Amazon Inspector Classic ou verificar se o agente está em execução). Visualize o status do seu agente e verifique se ele está usando o proxy configurado.

Para desinstalar o agente do Amazon Inspector Classic

Para desinstalar o agente

1. Conecte-se à instância do EC2, que está executando um sistema operacional baseado em Windows, da qual você deseja desinstalar o agente do Amazon Inspector Classic.

   > **Note**
   >
   > Para obter mais informações sobre os sistemas operacionais compatíveis com o Amazon Inspector Classic, consulte Sistemas operacionais e regiões compatíveis com o Amazon Inspector Classic.

2. Na sua instância do EC2, navegue até Painel de controle, Adicionar ou remover programas.
3. Na lista de programas instalados, selecione AWS Agent e, em seguida, selecione Desinstalar.

(Opcional) Verifique a assinatura do script de instalação do agente do Amazon Inspector Classic em sistemas operacionais baseados em Linux

Este tópico descreve o processo recomendado de verificação da validade do script de instalação do agente do Amazon Inspector Classic para sistemas operacionais baseados em Linux.

Sempre que baixar um aplicativo da Internet, recomendamos que você autentique a identidade do fornecedor do software e verifique se o aplicativo não foi alterado ou corrompido desde que foi publicado. Isso protege você contra a instalação de uma versão do aplicativo que contenha um vírus ou outro código mal-intencionado.

Se depois de executar as etapas neste tópico, você determinar que o software do agente do Amazon Inspector Classic está alterado ou corrompido, NÃO execute o arquivo de instalação. Em vez disso, entre em contato com AWS Support.

Os arquivos do agente Amazon Inspector Classic para sistemas operacionais baseados em Linux são assinados usando `GnuPG`, uma implementação de código aberto do padrão Pretty Good Privacy (OpenPGP) para assinaturas digitais seguras. `GnuPG` (também conhecido como `GPG`) fornece autenticação e verificação de integridade por meio de uma assinatura digital. O Amazon EC2 publica uma chave pública e assinaturas que você pode usar para verificar as ferramentas da CLI

do Amazon EC2 baixadas. Para obter mais informações sobre PGP e GnuPG (GPG), consulte http://www.gnupg.org.

A primeira etapa é estabelecer confiança com o fornecedor do software. Faça download da chave pública do fornecedor do software, verifique se o proprietário da chave pública é quem afirma ser e, em seguida, adicione a chave pública ao seu keyring. O keyring é um conjunto de chaves públicas conhecidas. Após estabelecer a autenticidade da chave pública, você pode usá-la para verificar a assinatura do aplicativo.

Tópicos

Como instalar as ferramentas do GPG

Se o seu sistema operacional for Linux ou Unix, as ferramentas do GPG já estarão instaladas. Para testar se as ferramentas estão instaladas no sistema, digite gpg em um prompt de comando. Se as ferramentas do GPG estiverem instaladas, um prompt de comando do GPG será exibido. Se as ferramentas do GPG não estiverem instaladas, uma mensagem de erro será exibida informando que o comando não pode ser encontrado. Você pode instalar o pacote GnuPG a partir de um repositório.

Para instalar as ferramentas do GPG no Linux baseado em Debian

- Em um terminal, execute o comando a seguir: apt-get install gnupg.

Para instalar as ferramentas do GPG no Linux baseado em Red Hat

- Em um terminal, execute o comando a seguir: yum install gnupg.

Como autenticar e importar a chave pública

A próxima etapa do processo é autenticar a chave pública do Amazon Inspector Classic e adicioná-la como uma chave confiável ao seu keyring GPG.

Para autenticar e importar a chave pública do Amazon Inspector Classic

1. Obtenha uma cópia de nossa compilação de chave pública do GPG de uma das seguintes maneiras:

   - Baixe em https://d1wk0tztpsntt1.cloudfront.net/linux/latest/inspector.gpg.
   - Copie a chave do texto abaixo e cole-a em um arquivo chamado `inspector.gpg`. Certifique-se de incluir tudo o que está a seguir:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.18 (GNU/Linux)

mQINBFYDlfEBEADFpfNt/mdCtsmfDoga+PfHY9bdXAD68yhp2m9NyH3BOzle/MXI
8siNfoRgzDwuWnIaezHwwLWkDw2paRxp1NMQ9qRe8Phq0ewheLrQu95dwDgMcw90
gf9m1iKVHjdVQ9qNHlB2OFknPDxMDRHcrmlJYDKYCX3+MODEHnlK25tIH2KWezXP
FPSU+TkwjLRzSMYH1L8IwjFUIIi78jQS9a31R/cOl4zuC5fOVghYlSomLI8irfoD
JSa3csVRujSmOAf9o3beiMR/kNDMpgDOxgiQTu/Kh39cl6o8AKe+QKK48kqO7hra
h1dpzLbfeZEVU6dWMZtlUksG/zKxuzD6d8vXYH7Z+x09POPFALQCQQMC3WisIKgj
zJEFhXMCCQ3NLC3CeyMq3vP7MbVRBYE7t3d2uDREkZBgIf+mbUYfYPhrzy0qT9Tr
PgwcnUvDZuazxuuPzucZGOJ5kbptat3DcUpstjdkMGAId3JawBbps77qRZdA+swr
o9o3jbowgmf0y5ZS6KwvZnC6XyTAkXy2io7mSrAIRECrANrzYzfp5v7uD7w8Dk0X
1OrfOm1VufMzAyTu0YQGBWaQKzSB8tCkvFw54PrRuUTcV826XU7SIJNzmNQo58uL
bKyLVBSCVabfs0lkECIesq8PT9xMYfQJ421uATHyYUnFTU2TYrCQEab7oQARAQAB
tCdBbWF6b24gSW5zcGVjdG9yIDxpbnNwZWN0b3JAYW1hem9uLmNvbT6JAjgEEwEC
ACIFAlYDlfECGwMGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJECR0CWBYNgQY
8yUP/2GpIl40f3mKBUiSTe0XQLvwiBCHmY+V9fOuKqDTinxssjEMCnz0vsKeCZF/
L35pwNa/oW0OJa8D7sCkKG+8LuyMpcPDyqptLrYPprUWtz2+qLCHgpWsrku7ateF
x4hWS0jUVeHPaBzI9V1NTHsCx9+nbpWQ5Fk+7VJI8hbMDY7NQx6fcse8WTlP/0r/
HIkKzzqQQaaOf5t9zc5DKwi+dFmJbRUyaq22xs8C81UODjHunhjHdZ21cnsgk91S
fviuaum9aR4/uVIYOTVWnjC5J3+VlczyUt5FaYrrQ5ov0dM+biTUXwve3X8Q85Nu
DPnO/+zxb7Jz3QCHXnuTbxZTjvvl60Oi8//uRTnPXjz4wZLwQfibgHmk1++hzND7
wOYA02Js6v5FZQlLQAod7q2wuA1pq4MroLXzziDfy/9ea8B+tzyxlmNVRpVZY4Ll
DOHyqGQhpkyV3drjjNZlEofwbfu7m6ODwsgMl5ynzhKklJzwPJFfB3mMc7qLi+qX
MJtEX8KJ/iVUQStHHAG7daL1bxpWSI3BRuaHsWbBGQ/mcHBgUUOQJyEp5LAdg9Fs
VP55gWtF7pIqifiqlcfgG0Ov+A3NmVbmiGKSZvfrc5KsF/k43rCGqDx1RV6gZvyI
LfO9+3sEIlNrsMib0KRLDeBt3EuDsaBZgOkqjDhgJUesqiCy
=iEhB
-----END PGP PUBLIC KEY BLOCK-----
```

2. Em um prompt de comando no diretório onde você salvou inspector.gpg, use o seguinte comando para importar a chave pública do Amazon Inspector Classic para o seu chaveiro:

```
gpg --import inspector.gpg
```

O comando retorna resultados semelhantes a:

```
gpg: key 58360418: public key "Amazon Inspector <inspector@amazon.com>" imported
                   gpg: Total number processed: 1
                   gpg:               imported: 1  (RSA: 1)
```

Anote o valor da chave, ele será necessário na próxima etapa. No exemplo anterior, o valor da chave é `58360418`.

3. Verifique a impressão digital, executando o comando a seguir, substituindo chave-valor pelo valor da etapa anterior:

```
gpg --fingerprint key-value
```

Esse comando retorna resultados semelhantes a:

```
pub   4096R/58360418 2015-09-24
                Key fingerprint = DDA0 D4C5 10AE 3C20 6F46  6DC0 2474 0960 5836
 0418
                uid                  Amazon Inspector <inspector@amazon.com>
```

Além disso, a cadeia de caracteres da impressão digital deve ser idêntica a `DDA0 D4C5 10AE 3C20 6F46 6DC0 2474 0960 5836 0418` mostrado acima no exemplo anterior. Compare a impressão digital da chave retornada à publicada nesta página. Elas devem corresponder. Se elas não corresponderem, não instale o script de instalação do agente da Amazon Inspector Classic e entre em contato com AWS Support.

Verificar a assinatura do pacote

Depois de instalar as ferramentas `GPG`, autenticar e importar a chave pública do Amazon Inspector Classic e verificar se a chave pública é confiável, você estará pronto para verificar a assinatura do script de instalação.

Para verificar a assinatura do script de instalação

1. Em um prompt de comando, execute o comando a seguir para baixar o arquivo de assinatura do script de instalação:

   ```
   curl -O https://inspector-agent.amazonaws.com/linux/latest/install.sig
   ```

2. Verifique a assinatura executando o comando a seguir em um prompt de comando no diretório onde você salvou `install.sig` e o arquivo de instalação do Amazon Inspector Classic. Ambos os arquivos devem estar presentes.

   ```
   gpg --verify ./install.sig
   ```

   A saída deve parecer com algo semelhante ao seguinte:

   ```
   gpg: Signature made Thu 24 Sep 2015 03:19:09 PM UTC using RSA key ID 58360418
   gpg: Good signature from "Amazon Inspector <inspector@amazon.com>" [unknown]
   gpg: WARNING: This key is not certified with a trusted signature!
   gpg:          There is no indication that the signature belongs to the owner.
   Primary key fingerprint: DDA0 D4C5 10AE 3C20 6F46  6DC0 2474 0960 5836 0418
   ```

   Se a saída contiver a frase `Good signature from "Amazon Inspector <inspector@amazon.com>"`, isso significa que a assinatura foi confirmada com êxito e você pode dar continuidade à execução do script de instalação do Amazon Inspector Classic.

   Se a saída inclui a frase `BAD signature`, verifique se você executou o procedimento corretamente. Se você continuar a receber essa resposta, não execute o arquivo de instalação que baixou anteriormente e entre em contato com AWS Support.

Veja a seguir os detalhes sobre as advertências que talvez sejam exibidas:

- AVISO: esta chave não está certificada com uma assinatura confiável! Não há indicação de que a assinatura pertença ao proprietário. Isso se refere ao seu nível pessoal de confiança de que você tem uma chave pública autêntica para o Amazon Inspector Classic. A situação ideal seria você visitar um escritório da AWS e receber uma chave em pessoa. No entanto, é mais frequente você baixá-la de um site. Nesse caso, o site é uma AWS.
- gpg: em última análise, nenhuma chave confiável encontrada. Isso significa que a chave específica não é "essencialmente confiável" (por você ou por outras pessoas que você confia).

Para obter mais informações, consulte http://www.gnupg.org.

(Opcional) Verifique a assinatura do script de instalação do agente do Amazon Inspector Classic em sistemas operacionais baseados em Windows

Este tópico descreve o processo recomendado de verificação da validade do script de instalação do agente do Amazon Inspector Classic para sistemas operacionais baseados em Windows.

Sempre que baixar um aplicativo da Internet, recomendamos que você autentique a identidade do fornecedor do software e verifique se o aplicativo não foi alterado ou corrompido desde que foi publicado. Isso protege você contra a instalação de uma versão do aplicativo que contenha um vírus ou outro código mal-intencionado.

Se depois de executar as etapas neste tópico, você determinar que o software do agente do Amazon Inspector Classic está alterado ou corrompido, NÃO execute o arquivo de instalação. Em vez disso, entre em contato com AWS Support.

Para verificar a validade do script de instalação do agente baixado em sistemas operacionais Windows, você deve certificar-se de que o thumbprint do certificado do assinante do Amazon Services LLC seja igual a este valor:

E8 83 C5 3A F7 8C BA 7C F5 A2 47 E9 B8 86 FC E9 68 EE 0B 36

Para verificar esse valor, execute o procedimento a seguir:

1. Clique com o botão direito do mouse no `AWSAgentInstall.exe` baixado e abra a janela Properties (Propriedades).
2. Escolha a guia Assinaturas digitais.
3. Em Lista de assinaturas, escolha Amazon Web Services, Inc. e, em seguida, escolha Detalhes.
4. Escolha a guia Geral, se ainda não estiver selecionada, e escolha Visualizar certificado.
5. Selecione a guia Details (Detalhes) e All (Todos) na lista suspensa Show (Exibir), se ela ainda não estiver selecionada.
6. Role para baixo até ver o campo Thumbprint e, em seguida, escolha Thumbprint. Isso exibe todo o valor da impressão digital na janela inferior.

    - Se o valor da impressão digital na janela inferior for idêntico a este valor:

E8 83 C5 3A F7 8C BA 7C F5 A2 47 E9 B8 86 FC E9 68 EE 0B 36

o script de instalação do agente baixado é autêntico e pode ser instalado com segurança.

- Se o valor da impressão digital na janela de detalhes inferior não for idêntico ao valor acima, não execute `AWSAgentInstall.exe`.

Destinos de avaliação do Amazon Inspector Classic

Você pode usar o Amazon Inspector Classic para avaliar se os destinos de avaliação AWS (suas coleções de recursos AWS) têm possíveis problemas de segurança que precisam ser resolvidos.

> **Important**
>
> No momento, os destinos de avaliação podem consistir somente em instâncias do EC2 executadas em uma série de sistemas operacionais compatíveis. Para obter informações sobre os sistemas operacionais e as regiões da AWS compatíveis, consulte the section called “Sistemas operacionais e regiões compatíveis”.

> **Note**
>
> Para obter mais informações sobre o lançamento de instâncias do EC2, consulte a Documentação do Amazon Elastic Compute Cloud.

Tópicos

Recursos de marcação para criar um destino de avaliação

Para criar um destino de avaliação para ser avaliado pelo Amazon Inspector Classic, comece marcando as instâncias do EC2 que você quer incluir no destino. Tags são palavras ou frases que atuam como metadados para identificar e organizar suas instâncias e outros recursos AWS. O Amazon Inspector Classic usa as tags que você cria para identificar as instâncias que pertencem a sua meta.

Cada tag AWS consiste em um par de chave e valor de sua escolha. Por exemplo, você pode escolher chamar sua chave de "Nome" e seu valor "MinhaPrimeiraInstância". Depois de marcar

as instâncias, você usa o console do Amazon Inspector Classic para adicioná-las ao destino de avaliação. Não é necessário que as instâncias correspondam a mais de um par de chave-valor da tag.

Quando você marca as instâncias do EC2 para criar destinos de avaliação, você pode criar suas próprias chaves de tag personalizadas ou usar chaves de tags criadas por outros usuários na mesma conta AWS. Você também pode usar as chaves de tag que o AWS cria automaticamente. Por exemplo, o AWS cria automaticamente uma chave de tag Nome para as instâncias EC2 que você inicializa.

Você pode adicionar tags às instâncias EC2 ao criá-las ou pode adicionar, alterar ou remover as tags uma de cada vez na página do console de cada instância do EC2. Você também pode adicionar tags a várias instâncias do EC2 de uma só vez usando o Tag Editor.

Para obter mais informações, consulte o Tag Editor. Para mais informações sobre a marcação de instâncias do EC2, consulte Recursos e tags.

Limites do destino de avaliação do Amazon Inspector Classic

Você pode criar até 50 destinos de avaliação por conta AWS. Para obter mais informações, consulte Limites do serviço do Amazon Inspector Classic.

Como criar um destino de avaliação

Você pode usar o console do Amazon Inspector Classic para criar destinos de avaliação.

Para criar um destino de avaliação

1. Faça login no AWS Management Console e abra o console do Amazon Inspector Classic em https://console.aws.amazon.com/inspector/.
2. No painel de navegação, escolha Destinos de avaliação e, em seguida, Criar.
3. Em Nome, insira um nome para o destino de avaliação.
4. Faça um dos seguintes procedimentos:
   - Para incluir todas as instâncias do EC2 na conta AWS e a região neste destino de avaliação, selecione a caixa Todas as instâncias.

> **Note**
>
> O limite para o número máximo de agentes que podem ser incluídos em uma execução de avaliação se aplica quando você usa essa opção. Para obter mais informações, consulte Limites do serviço do Amazon Inspector Classic.

- Para escolher as instâncias do EC2 que você quiser incluir no destino de avaliação, em Usar tags, insira os nomes de chaves de tag e os pares de chave e valor.

5. (Opcional) Ao criar um novo destino, você pode marcar a caixa de seleção Instalar agentes para instalar o agente em todas as instâncias do EC2 nesse destino. Para usar essa opção, as instâncias do EC2 devem ter o SSM Agent instalado e uma função do IAM que permita o Run Command. O SSM Agent é instalado, por padrão, em instâncias do Windows no Amazon EC2 e no Amazon Linux. O Amazon EC2 Systems Manager requer uma função do IAM para instâncias do EC2 que processará comandos e uma função separada para os usuários que estejam executando comandos. Para obter mais informações, consulte Instalação e configuração do SSM Agent e Configuração de funções de segurança para System Manager.

> **Important**
>
> Se uma instância do EC2 já tem um agente em execução, o uso dessa opção substitui o agente que está em execução na instância atualmente pela versão mais recente dele.

> **Note**
>
> Para os destinos de avaliação existentes, você pode selecionar o botão Instalar agentes com o Executar Comando para instalar o agente em todas as instâncias do EC2 nesse destino.

> **Note**
>
> Você também pode instalar o agente em várias instâncias do EC2 (instâncias baseadas no Linux e no Windows com o mesmo comando) remotamente usando o Executar Comando do Systems Manager. Para obter mais informações, consulte Instalar o agente

do Amazon Inspector em várias instâncias do EC2 usando o Executar Comando do Systems Manager.

6. Escolha Save (Salvar).

> **Note**
>
> Você pode usar o botão Visualizar destino na página Destinos de avaliação para analisar todas as instâncias do EC2 incluídas no destino de avaliação. Para cada instância do EC2, você pode analisar o nome do host, o ID da instância, o endereço IP e, se aplicável, o status do agente. O status do agente pode ter os seguintes valores: SAUDÁVEL, POUCO SAUDÁVEL e DESCONHECIDO. O Amazon Inspector Classic exibe um status DESCONHECIDO quando não consegue determinar se há um agente em execução na instância do EC2.

Como excluir um destino de avaliação

Para excluir um destino de avaliação, siga o procedimento a seguir.

Para excluir um destino de avaliação

- Na página Destinos de avaliação, selecione a meta que você deseja excluir e selecione Excluir. Quando a confirmação for solicitada, selecione Yes (Sim).

> **Important**
>
> Ao excluir um destino de avaliação, todos os modelos de avaliação, execuções de avaliação, descobertas e versões dos relatórios associados ao destino também são excluídos.

Você também pode excluir um destino de avaliação usando a API `DeleteAssessmentTarget`.

Pacotes de regras e regras do Amazon Inspector Classic

Você pode usar o Amazon Inspector Classic para avaliar seus destinos de avaliação (coleções de recursos da AWS) para encontrar possíveis problemas de segurança e vulnerabilidades. O Amazon Inspector Classic compara o comportamento e a configuração de segurança dos destinos de avaliação a pacotes de regras de segurança selecionados. No contexto do Amazon Inspector Classic, uma regra é uma verificação de segurança que o Amazon Inspector Classic executa durante uma execução de avaliação.

No Amazon Inspector Classic, as regras são agrupadas em pacotes de regras distintos por categoria, gravidade ou definição de preço. Esse recurso oferece opções para os tipos de análises que você pode executar. Por exemplo, o Amazon Inspector Classic oferece um grande número de regras que você pode usar para avaliar seus aplicativos. Mas você pode querer incluir um pequeno subconjunto das regras disponíveis para concentrar-se em uma área específica que causa preocupação ou para descobrir problemas de segurança específicos. Empresas com grandes departamentos de TI podem querer determinar se o seu aplicativo está exposto a qualquer ameaça de segurança. Outras podem querer se concentrar somente nos problemas com nível de gravidade Alto.

- Níveis de gravidade para regras no Amazon Inspector Classic
- Pacotes de regras no Amazon Inspector Classic

Níveis de gravidade para regras no Amazon Inspector Classic

Cada regra do Amazon Inspector Classic tem um nível de gravidade atribuído. Isso reduz a necessidade de priorizar uma regra sobre outra nas suas análises. Isso também pode ajudar você a determinar sua resposta quando uma regra destaca um potencial problema.

Os níveis Alto, Médio e Baixo indicam um problema de segurança que pode resultar no comprometimento da confidencialidade, integridade e disponibilidade das informações no destino de avaliação. Os níveis são diferenciados pela probabilidade de o problema resultar em um comprometimento e pela urgência em corrigi-lo.

O nível Informativo simplesmente destaca detalhes das configurações de segurança do destino de avaliação.

Aqui estão as formas recomendadas de responder aos problemas com base em sua gravidade:

- Alto — Problemas de alta gravidade são extremamente urgentes. O Amazon Inspector Classic recomenda que você trate esse problema de segurança como uma emergência e implemente uma correção imediata.
- Média — Problemas de média gravidade são um tanto urgentes. O Amazon Inspector Classic recomenda que você corrija esse problema na próxima oportunidade possível, por exemplo, durante a próxima atualização de serviço.
- Baixo — Problemas de baixa gravidade são menos urgentes. O Amazon Inspector Classic recomenda que você corrija esse problema como parte de uma de suas futuras atualizações de serviço.
- Informativo — Esses problemas são puramente informativos. Com base nos objetivos da empresa e da organização, você pode simplesmente anotar essas informações ou usá-las para melhorar a segurança do destino de avaliação.

Pacotes de regras no Amazon Inspector Classic

Uma avaliação do Amazon Inspector pode usar qualquer combinação dos seguintes pacotes de regras:

Avaliações de rede:

- Acessibilidade de rede

Avaliações de host:

- Vulnerabilidades e exposições comuns
- Referências de segurança da CIS (Center for Internet Security)
- Práticas recomendadas de segurança para o Amazon Inspector Classic

Acessibilidade de rede

As regras no pacote de regras de acessibilidade de rede analisam suas configurações de rede para encontrar vulnerabilidades de segurança de suas instâncias do EC2. As descobertas que o Amazon Inspector gera também fornecem orientações sobre como restringir o acesso que não é seguro.

O pacote de regras de acessibilidade de rede usa a tecnologia mais recente da iniciativa AWS Provable Security.

As descobertas geradas por essas regras mostram se as portas podem ser acessadas pela Internet por meio de um gateway de Internet (incluindo instâncias atrás de Application Load Balancers ou Classic Load Balancers), uma conexão de emparelhamento de VPC ou uma VPN por meio de um gateway virtual. Esses resultados também destacam configurações de rede que permitem acessos potencialmente mal-intencionados, como grupos de segurança, IGWs ACLs, e assim por diante.

Essas regras ajudam a automatizar o monitoramento de suas redes da AWS e a identificar onde o acesso à rede para sua instância do EC2 pode estar configurado incorretamente. Incluindo esse pacote em sua execução de avaliação, você pode implementar as verificações de segurança de rede sem a necessidade de instalar scanners e enviar pacotes, que é complexo e caro para manter, especialmente em conexões de emparelhamento de VPCs e VPNs.

> **Important**
>
> Um agente Amazon Inspector Classic não é necessário para avaliar suas instâncias do EC2 com esse pacote de regras. No entanto, um agente instalado pode fornecer informações sobre a presença de todos os processos de escuta nas portas. Não instale um agente em um sistema operacional incompatível com o Amazon Inspector Classic. Se um agente estiver presente em uma instância que executa um sistema operacional incompatível, o pacote de regras de acessibilidade de rede não funcionará nessa instância.

Para ter mais informações, consulte Pacotes de regras do Amazon Inspector Classic para sistemas operacionais compatíveis.

Configurações analisadas

Regras de Acessibilidade de rede analisam a configuração das seguintes entidades de vulnerabilidades:

- Instâncias do Amazon EC2
- Application Load Balancers
- Conexão direta
- Elastic Load Balancers
- Interfaces de rede elástica
- Gateways da Internet (IGWs)
- Network Access Control Lists (ACLs)

- Tabelas de rotas
- Grupos de segurança (SGs)
- Subredes
- Virtual Private Clouds (VPCs)
- Virtual Private Gateways (VGWs)
- Conexões de emparelhamento da VPC

Rotas de acessibilidade

Regras de acessibilidade de rede verificam as seguintes rotas de acessibilidade, que corresponde às formas nas quais suas portas podem ser acessadas de fora de sua VPC:

- **`Internet`** - Gateways da Internet (incluindo Application Load Balancers e Classic Load Balancers)
- **`PeeredVPC`** - Conexões de emparelhamento de VPC
- **`VGW`** - Gateways privados virtuais

Tipos de descoberta

Uma avaliação que inclui pacote de regras de Acessibilidade de rede pode retornar os seguintes tipos de descobertas para cada rota de acessibilidade:

- `RecognizedPort`
- `UnrecognizedPortWithListener`
- `NetworkExposure`

`RecognizedPort`

Uma porta que normalmente é usada para um serviço é acessível. Se um agente estiver presente na instância do EC2 de destino, a descoberta gerada também indicará se há um processo de escuta ativo na porta. Descobertas desse tipo recebem uma gravidade com base no impacto de segurança do serviço conhecido:

- **`RecognizedPortWithListener`** – Uma porta reconhecida é alcançada externamente da Internet pública por meio de um componente de rede específico, e um processo está escutando na porta.
- **`RecognizedPortNoListener`** – Uma porta é acessível externamente da Internet pública por meio de um componente de rede específico, e não há processos escutando na porta.
- **`RecognizedPortNoAgent`** – Uma porta é externamente acessível pela Internet pública por meio de um componente de rede específico. A presença de um processo de escuta na porta não pode ser determinada sem instalar um agente na instância de destino.

A tabela a seguir mostra uma lista de portas reconhecidas:

Serviço	Portas TCP	Portas UDP
SMB	445	445
NetBIOS	137, 139	137, 138
LDAP	389	389
LDAP por TLS	636	
LDAP de catálogo global	3268	
LDAP de catálogo global sobre TLS	3269	
NFS	111, 2049, 4045, 1110	111, 2049, 4045, 1110
Kerberos	88, 464, 543, 544, 749, 751	88, 464, 749, 750, 751, 752
RPC	111, 135, 530	111, 135, 530
WINS	1512, 42	1512, 42
DHCP	67, 68, 546, 547	67, 68, 546, 547
Syslog	601	514

Serviço	Portas TCP	Portas UDP
Serviços de impressão	515	
Telnet	23	23
FTP	21	21
SSH	22	22
RDP	3389	3389
MongoDB	27017, 27018, 27019, 28017	
SQL Server	1433	1434
MySQL	3306	
PostgreSQL	5432	
Oracle	1521, 1630	
Elasticsearch	9300, 9200	
HTTP	80	80
HTTPS	443	443

`UnrecogizedPortWithListener`

Uma porta que não esteja listada na tabela anterior deve ser acessível e ter um processo de escuta ativo. Como as descobertas desse tipo mostram informações sobre processos de escuta, elas só podem ser geradas quando um agente do Amazon Inspector está instalado na instância do EC2 de destino. As descobertas deste tipo são determinadas como de gravidade Baixa.

`NetworkExposure`

As descobertas desse tipo mostram informações agregadas nas portas que estão disponíveis em sua instância do EC2. Para cada combinação de interfaces de rede elástica e grupos de segurança

em uma instância do EC2, essas descobertas mostram o conjunto acessível de intervalos de portas TCP e UDP. As descobertas deste tipo tem a gravidade de Informação.

Vulnerabilidades e exposições comuns

As regras deste pacote ajudam a verificar se as instâncias do EC2 nos seus destinos de avaliação estão expostas a vulnerabilidades e exposições comuns (common vulnerabilities and exposures - CVEs). Os ataques podem explorar vulnerabilidades sem correção e comprometer a confidencialidade, a integridade ou a disponibilidade de seu serviço ou de seus dados. O sistema CVE fornece um método de referência a informações conhecidas publicamente sobre vulnerabilidades e exposições de segurança. Para obter mais informações, consulte https://cve.mitre.org/.

Se uma determinada CVE for exibida em uma descoberta produzida por uma avaliação do Amazon Inspector Classic, você poderá pesquisar em https://cve.mitre.org/ o ID do CVE (por exemplo, **`CVE-2009-0021`**). Os resultados da pesquisa podem fornecer informações detalhadas sobre o CVE, sua severidade e como remediá-lo.

Para o pacote de regras Common Vulnerabilities & Exploits (CVE), o Amazon Inspector mapeou a pontuação básica do CVSS e os níveis de gravidade do ALAS fornecidos:

Gravidade do Amazon Inspector	Pontuação básica do CVSS	Gravidade do ALAS (se o CVSS não for pontuado)
Alta	>= 5	Crítico ou importante
Médio	< 5 and >= 2,1	Médio
Baixo	< 2.1 and >= 0,8	Baixo
Informativo	< 0,8	N/D

As regras incluídas neste pacote ajudam você a avaliar se as suas instâncias do EC2 estão expostas às CVEs nas seguintes listas regionais:

- Leste dos EUA (Norte da Virgínia)
- Leste dos EUA (Ohio)
- Oeste dos EUA (Norte da Califórnia)

- Oeste dos EUA (Oregon)
- UE (Irlanda)
- UE (Frankfurt)
- UE (Londres)
- UE (Estocolmo)
- Ásia-Pacífico (Tóquio)
- Ásia-Pacífico (Seul)
- Ásia Pacífico (Mumbai)
- Ásia-Pacífico (Sydney)
- AWS GovCloud West (EUA)
- AWS GovCloud Leste (EUA)

O pacote de regras de CVE é atualizado regularmente. Essa lista contém as CVEs que estão incluídas nas execuções de avaliação que ocorrem ao mesmo tempo em que a lista é recuperada.

Para ter mais informações, consulte Pacotes de regras do Amazon Inspector Classic para sistemas operacionais compatíveis.

Referências de segurança da CIS (Center for Internet Security)

O programa CIS Security Benchmarks fornece as melhores práticas do setor bem definidas, imparciais e baseadas em consenso para ajudar as organizações a avaliar e melhorar sua segurança. AWS é uma empresa membro do CIS Security Benchmarks. Para obter uma lista de certificações do Amazon Inspector Classic, consulte a página da Amazon Web Services no site da CIS.

No momento, o Amazon Inspector Classic oferece os seguintes pacotes de regras com certificação CIS para ajudar a estabelecer posturas de configuração seguras para os seguintes sistemas operacionais:

Amazon Linux

- `CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 1`
- `CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 2`

- CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 1
- CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 2
- CIS Benchmark for Amazon Linux 2014.09-2015.03 v1.1.0 Level 1

CentOS Linux

- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Server
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Server
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Workstation
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Workstation
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 1 Server
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 1 Workstation
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 2 Workstation

Red Hat Enterprise Linux

- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 1 Server
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2. Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Workstation

Ubuntu

- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Workstation
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Workstation
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 2 Workstation

Windows

- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 1 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 2 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 1 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 2 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Next Generation Windows Security Profile)

- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 1 Domain Controller Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 2 Domain Controller Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 1 Member Server Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 2 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 2 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Domain Controller Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 2 Domain Controller Profile)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Domain Controller Profile)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Member Server Profile)

Se determinada referência da CIS for exibida em uma descoberta produzida por uma execução de avaliação do Amazon Inspector Classic, você poderá fazer download de um PDF com a descrição detalhada da referência em https://benchmarks.cisecurity.org/ (é necessário fazer o registro gratuito). O documento de referência da CIS fornece informações detalhadas sobre ela, sua severidade e como remediá-la.

Para ter mais informações, consulte Pacotes de regras do Amazon Inspector Classic para sistemas operacionais compatíveis.

Práticas recomendadas de segurança para o Amazon Inspector Classic

Use as regras do Amazon Inspector Classic para ajudar a determinar se os seus sistemas estão configurados de forma segura.

> **Important**
>
> Atualmente, você pode incluir em seus destinos de avaliação as instâncias do EC2 que executam sistemas operacionais baseados em Linux ou Windows.
> Durante uma execução de avaliação, as regras descritas nesta seção geram descobertas somente para as instâncias do EC2 que estão executando um sistema operacional Linux. As regras não geram descobertas para instâncias do EC2 que estão executando um sistema operacional Windows.
> Para obter mais informações, consulte Pacotes de regras do Amazon Inspector Classic para sistemas operacionais compatíveis.

Tópicos

Desabilitar o login raiz pelo SSH

Essa regra ajuda a determinar se o daemon do SSH está configurado para permitir o login na instância do EC2 como raiz.

Gravidade

Médio

Descoberta

Há uma instância do EC2 em seu destino de avaliação que está configurada para permitir que os usuários façam login com credenciais raiz via SSH. Isso aumenta a probabilidade de sucesso de um ataque de força bruta.

Resolução

Recomendamos que você configure sua instância do EC2 para evitar logins na conta raiz via SSH. Em vez disso, faça login como um usuário não raiz e use o `sudo` para aumentar privilégios quando necessário. Para desabilitar os logins na conta raiz via SSH, defina `PermitRootLogin` como no no arquivo `/etc/ssh/sshd_config` e reinicie `sshd`.

Suporte somente ao SSH versão 2

Essa regra ajuda a determinar se as instâncias EC2 estão configuradas para oferecer suporte à versão 1 do protocolo SSH.

Gravidade

Médio

Descoberta

Uma instância do EC2 em seu destino de avaliação que está configurada para oferecer suporte ao SSH-1, que contém falhas de projeto inerentes que reduzem significativamente a segurança.

Resolução

Recomendamos que você configure as instâncias do EC2 no destino de avaliação para oferecer suporte somente ao SSH-2 e posterior. Para o OpenSSH, você pode fazer isso, definindo `Protocol 2` no arquivo `/etc/ssh/sshd_config`. Para obter mais informações, consulte `man sshd_config`.

Desabilitar a autenticação de senha por SSH

Essa regra ajuda a determinar se as instâncias do EC2 estão configuradas para oferecer suporte à autenticação de senha via protocolo SSH.

Gravidade

Médio

Descoberta

Uma instância do EC2 em seu destino de avaliação está configurada para oferecer suporte à autenticação de senha via SSH. A autenticação de senhas é suscetível a ataques de força bruta e deve ser desativada em favor da autenticação baseada em chave sempre que possível.

Resolução

Recomendamos que você desative a autenticação de senha via SSH nas instâncias do EC2 e ative o suporte à autenticação baseada em chave em seu lugar. Isso reduz significativamente a probabilidade de sucesso de um ataque de força bruta. Para obter mais informações, consulte https://aws.amazon.com/articles/1233/. Se a autenticação de senha tiver suporte, é importante restringir o acesso ao servidor SSH a endereços IP confiáveis.

Configurar a duração máxima da senha

Essa regra ajuda a determinar se a duração máxima das senhas está configurada nas instâncias do EC2.

Gravidade

Médio

Descoberta

Uma instância do EC2 em seu destino de avaliação não está configurada para a duração máxima das senhas.

Resolução

Se estiver usando senhas, recomendamos que você configure uma duração máxima para elas em todas as instâncias do EC2 em seu destino de avaliação. Isso requer que os usuários alterem as senhas regularmente e reduz as chances de sucesso de um ataque para adivinhá-las. Para corrigir o problema para usuários existentes, use o comando chage. Para configurar a duração máxima das senhas para todos os usuários, edite o campo `PASS_MAX_DAYS` no arquivo `/etc/login.defs`.

Configurar o tamanho mínimo da senha

Essa regra ajuda a determinar se o tamanho mínimo das senhas está configurado nas instâncias do EC2.

Gravidade

Médio

Descoberta

Uma instância do EC2 em sseu destino de avaliação não está configurada para o tamanho mínimo das senhas.

Resolução

Se estiver usando senhas, recomendamos que você configure um tamanho mínimo para as senhas em todas as instâncias do EC2 em seu destino de avaliação. Impor um tamanho mínimo de senha reduz o risco de sucesso de um ataque para adivinhá-las. Você pode fazer isso usando as opções a seguir no `pwquality.conf` arquivo: `minlen`. Para mais informações, consulte https://linux.die.net/man/5/pwquality.conf.

Se `pwquality.conf` não estiver disponível na instância, você pode definir a opção `minlen` usando o módulo `pam_cracklib.so`. Para obter mais informações, consulte `man pam_cracklib`.

A opção `minlen` deve ser definida como 14 ou maior.

Configurar a complexidade da senha

Essa regra ajuda a determinar se um mecanismo de complexidade de senha está configurado nas instâncias do EC2.

Gravidade

Médio

Descoberta

Nenhum mecanismo de complexidade de senha ou de restrição está configurado nas instâncias do EC2 em seu destino de avaliação. Isso permite que os usuários definam senhas simples, o que aumenta as chances de usuários não autorizados obterem acesso às contas e usá-las indevidamente.

Resolução

Se estiver usando senhas, recomendamos que você configure todas as instâncias do EC2 no seu destino de avaliação para exigir um nível de complexidade de senha. Você pode fazer isso usando as opções a seguir no arquivo `pwquality.conf`: `lcredit`, `ucredit`, `dcredit` e `ocredit`. Para mais informações, consulte https://linux.die.net/man/5/pwquality.conf .

Se `pwquality.conf` não estiver disponível na instância, você pode definir as opções `lcredit`, `ucredit`, `dcredit` e `ocredit` usando o módulo `pam_cracklib.so`. Para obter mais informações, consulte `man pam_cracklib`.

O valor esperado para cada uma dessas opções é menor ou igual a -1, conforme mostrado abaixo:

```
lcredit <= -1, ucredit <= -1, dcredit<= -1, ocredit <= -1
```

Além disso, a opção `remember` deve ser definida como 12 ou superior. Para obter mais informações, consulte `man pam_unix`.

Habilitar ASLR

Esta regra ajuda a determinar se a randomização de layout do espaço de endereço (ASLR) está habilitada nos sistemas operacionais das instâncias do EC2 no seu destino de avaliação.

Gravidade

Médio

Descoberta

Uma instância do EC2 em seu destino de avaliação não tem ASLR ativada.

Resolução

Para melhorar a segurança do destino de avaliação, recomendamos que você habilite a ASLR nos sistemas operacionais de todas as instâncias EC2 na meta, executando echo 2 | sudo tee /proc/sys/kernel/randomize_va_space.

Habilitar DEP

Esta regra ajuda a determinar se a Prevenção de Execução de Dados (DEP) está habilitada nos sistemas operacionais das instâncias do EC2 no seu destino de avaliação.

> **Note**
>
> Essa regra não é compatível com instâncias do EC2 com processadores ARM.

Gravidade

Médio

Descoberta

Uma instância do EC2 em sseu destino de avaliação não tem a DEP ativada.

Resolução

Recomendamos que você ative a DEP nos sistemas operacionais de todas as instâncias do EC2 em seu destino de avaliação. Habilitar a DEP protege as instâncias contra comprometimentos de segurança usando técnicas de estouro de buffer.

Configurar permissões para os diretórios do sistema

Essa regra verifica as permissões nos diretórios do sistema que contêm binários e informações de configuração do sistema. Ele verifica que somente o usuário raiz (o usuário que faz login usando as credenciais da conta raiz) tenha permissões de gravação para esses diretórios.

Gravidade

Alto

Descoberta

Uma instância do EC2 em seu destino de avaliação contém um diretório do sistema de destino que é gravável por usuários não raiz.

Resolução

Para melhorar a segurança do seu destino de avaliação e evitar o escalonamento de privilégios por usuários locais mal-intencionados, configure todos os diretórios do sistema em todas as instâncias do EC2 no seu destino para serem graváveis apenas por usuários que fazem login usando credenciais de conta raiz.

Modelos de avaliação e execuções de avaliação do Amazon Inspector Classic

O Amazon Inspector Classic ajuda você a descobrir possíveis problemas de segurança usando regras de segurança para analisar seus AWS recursos. O Amazon Inspector Classic monitora e coleta dados comportamentais (telemetria) sobre seus recursos. Os dados incluem informações sobre o uso de canais seguros, tráfego de rede entre processos em execução e detalhes da comunicação com AWS os serviços. Em seguida, o Amazon Inspector Classic analisa e compara os dados em relação a um conjunto de pacotes de regras de segurança. Por fim, o Amazon Inspector Classic produz uma lista de descobertas que identificam possíveis problemas de segurança com diferentes graus de severidade.

Para começar, crie um destino de avaliação (uma coleção de recursos da AWS que você deseja que o Amazon Inspector Classic analise). Depois, crie um modelo de avaliação (um esquema que você usa para configurar sua avaliação). Você pode usar o modelo para iniciar uma execução de avaliação, que é o processo de monitoramento e análise que resulta em um conjunto de descobertas.

Tópicos

Modelos de avaliação do Amazon Inspector Classic

Um modelo de avaliação permite que você especifique uma configuração para sua execução de avaliação, incluindo o seguinte:

- Pacote de regras que o Amazon Inspector Classic usa para avaliar o destino de avaliação

- Duração da execução da avaliação - é possível definir a duração de uma execução de avaliação entre 3 minutos e 24 horas. Recomendamos definir a duração das execuções de avaliação como 1 hora.
- Os tópicos do Amazon SNS para os quais o Amazon Inspector Classic envia notificações sobre as descobertas e os estados da execução de avaliação
- Atributos específicos do Amazon Inspector Classic (pares de chave-valor) que você pode atribuir a descobertas que são geradas pela execução da avaliação que usa esse modelo de avaliação

Quando o Amazon Inspector Classic criar o modelo de avaliação, ele poderá ser marcado como qualquer outro recurso AWS . Para obter mais informações, consulte o Tag Editor. Marcar modelos de avaliação permite que você organize-os e supervisione melhor sua estratégia de segurança. Por exemplo, o Amazon Inspector Classic oferece um grande número de regras que você pode usar para avaliar seus destinos de avaliação. Você pode querer incluir vários subconjuntos das regras disponíveis em seus modelos de avaliação para áreas específicas que causam preocupação ou para descobrir problemas de segurança específicos. Marcar modelos de avaliação permite que você localize-os e execute-os rapidamente a qualquer momento, de acordo com sua estratégia de segurança e objetivos.

> **Important**
>
> Depois que criar um modelo de avaliação, você não poderá modificá-lo.

Limites dos modelos de avaliação do Amazon Inspector Classic

Você pode criar até 500 modelos de avaliação para cada AWS conta.

Para ter mais informações, consulte Limites do serviço do Amazon Inspector Classic.

Como criar um modelo de avaliação

Para criar um modelo de avaliação

1. Faça login AWS Management Console e abra o console do Amazon Inspector Classic em https://console.aws.amazon.com/inspector/.
2. No painel de navegação, escolha Assessment Templates (Modelos de avaliação) e, depois, escolha Create (Criar).

3. Em Name (Nome), insira um nome para o seu modelo de avaliação.
4. Em Nome do destino, selecione um destino de avaliação para analisar.

> **Note**
>
> Ao criar um modelo de avaliação, é possível usar o botão Visualizar destino na página Modelos de avaliação para analisar todas as instâncias do EC2 incluídas no destino de avaliação. Para cada instância do EC2, você pode analisar o nome do host, o ID da instância, o endereço IP e, se aplicável, o status do agente. O status do agente pode ter os seguintes valores: SAUDÁVEL, POUCO SAUDÁVEL e DESCONHECIDO. O Amazon Inspector Classic exibe um status DESCONHECIDO quando não consegue determinar se há um agente em execução na instância do EC2.
> Você também pode usar o botão Visualizar destino na página Modelos de avaliação para revisar as instâncias do EC2 que compõem os destinos de avaliação incluídos em modelos criados anteriormente.

5. Em Pacotes de regras, escolha um ou mais pacotes de regras para incluir no modelo de avaliação.
6. Em Duração, especifique a duração do modelo de avaliação.
7. (Opcional) Em Tópicos do SNS, especifique um tópico do SNS para o qual você deseja que o Amazon Inspector Classic envie notificações sobre estados de execução de avaliação e descobertas. O Amazon Inspector Classic pode enviar notificações do SNS sobre os seguintes eventos:

   - Uma execução de avaliação foi iniciada
   - Uma execução de avaliação foi concluída
   - O status de uma execução de avaliação foi alterado
   - Uma descoberta foi gerada

   Para obter mais informações sobre a configuração de um tópico do SNS, consulte Configurar um tópico do SNS para as notificações do Amazon Inspector Classic.
8. (Opcional) Em Tag, insira valores para Key (Chave) e Value (Valor). Você pode adicionar várias tags ao modelo de avaliação.
9. (Opcional) Em Atributos adicionados aos resultados, digite valores para Chave e Valor. O Amazon Inspector Classic aplica os atributos a todas as descobertas geradas pelo modelo

de avaliação. Você pode adicionar vários atributos ao modelo de avaliação. Para obter mais informações sobre as descobertas e a marcação das descobertas, consulte Descobertas do Amazon Inspector Classic.

10. (Opcional) Para configurar uma programação para as execuções de avaliação usando esse modelo, marque a caixa de seleção Set up recurring assessment runs once every <number_of_days>, starting now (Configurar execuções de avaliação recorrentes uma vez a cada <number_of_days>, a partir de agora) e especifique o padrão de recorrência (número de dias) usando as setas para cima e para baixo.

> **Note**
>
> Quando você usa essa caixa de seleção, o Amazon Inspector Classic cria automaticamente uma regra do Amazon CloudWatch Events para o cronograma de execuções de avaliação que você está configurando. Em seguida, o Amazon Inspector Classic também cria automaticamente uma função do IAM chamada. `AWS_InspectorEvents_Invoke_Assessment_Template` Essa função permite que CloudWatch os Eventos façam chamadas de API para os recursos do Amazon Inspector Classic. Para obter mais informações, consulte O que é Amazon CloudWatch Events? e usando políticas baseadas em recursos para CloudWatch eventos.

> **Note**
>
> Você também pode configurar execuções de avaliação automáticas por meio de uma função do AWS Lambda . Para ter mais informações, consulte Configurar execuções de avaliação automáticas por meio de uma função do Lambda.

11. Escolha Criar e executar ou Criar.

Como excluir um modelo de avaliação

Para excluir um modelo de avaliação, siga o procedimento a seguir.

Para excluir um modelo de avaliação

- Na página Modelos de avaliação, selecione o modelo que você deseja excluir e selecione Excluir. Quando a confirmação for solicitada, selecione Sim.

> **Important**
>
> Ao excluir um modelo de avaliação, todas as execuções de avaliação, descobertas e versões dos relatórios associados a esse modelo também são excluídas.

Você também pode excluir um modelo de avaliação usando a API `DeleteAssessmentTemplate`.

Execuções de avaliação

Depois que criar um modelo de avaliação, você poderá usá-lo para iniciar execuções de avaliação. Você pode iniciar várias execuções usando o mesmo modelo, desde que permaneça dentro do limite de execuções de cada AWS conta. Para ter mais informações, consulte Limites de execução da avaliação do Amazon Inspector Classic .

Se você usar o console do Amazon Inspector Classic, deverá iniciar a primeira execução do novo modelo de avaliação na página Modelos de avaliação. Depois de iniciada, você pode usar a página Execuções de avaliação para monitorar o progresso da execução. Use os botões Executar, Cancelar e Excluir para iniciar, cancelar ou excluir uma execução. É possível também visualizar os detalhes da execução, incluindo o ARN da execução, os pacotes de regras selecionados, as tags, os atributos que você aplicou e muito mais.

Para execuções subsequentes do modelo de avaliação, use os botões Executar, Cancelar e Excluir em uma das páginas Modelos de avaliação ou Execuções de avaliação.

Como excluir uma execução de avaliação

Para excluir uma execução de avaliação, siga o procedimento a seguir.

Para excluir uma execução

- Na página Assessment runs (Execuções de avaliação), selecione a execução que você deseja excluir e selecione Delete (Excluir). Quando a confirmação for solicitada, selecione Sim.

> **Important**
>
> Ao excluir uma execução, todas as descobertas e todas as versões do relatório dessa execução também são excluídas.

Você também pode excluir uma execução usando a API `DeleteAssessmentRun`.

Limites de execução da avaliação do Amazon Inspector Classic

Você pode criar até 50.000 execuções de avaliação para cada AWS conta.

Você pode ter várias execuções ocorrendo ao mesmo tempo, desde que as metas usadas para as execuções não contenham sobreposição de instâncias do EC2.

Para ter mais informações, consulte Limites do serviço do Amazon Inspector Classic.

Configurar execuções de avaliação automáticas por meio de uma função do Lambda

Se deseja configurar uma programação recorrente para a avaliação, você pode configurar o modelo de avaliação para executar automaticamente, criando uma função do Lambda por meio do console do AWS Lambda . Para obter mais informações, consulte Funções do Lambda.

Para configurar execuções automáticas de avaliação usando o AWS Lambda console, execute o procedimento a seguir.

Para configurar execuções automáticas por meio da função do Lambda

1. Faça login no AWS Management Console e abra o AWS Lambda console.
2. No painel de navegação, escolha Painel ou Funções e, em seguida, escolha Criar uma função do Lambda.
3. Na página Create function (Criar função), selecione Browse serverless app repository (Pesquisar no repositório de aplicativos sem servidor) e insira **`inspector`** no campo de busca.
4. Escolha o esquema inspector-scheduled-run.
5. Na página Revisar, configurar e implantar, configure uma programação recorrente para execuções automatizadas especificando um CloudWatch evento que aciona sua função. Para fazer isso, insira um nome e descrição da regra e selecione uma expressão de programação. A expressão de programação determina a frequência com que a execução ocorrerá, por exemplo, a cada 15 minutos ou uma vez por dia. Para obter mais informações sobre CloudWatch eventos e conceitos, consulte O que é Amazon CloudWatch Events?

   Se você marcar a caixa de seleção Enable trigger (Habilitar gatilho), a execução começará imediatamente depois que você concluir a criação da função. Execuções automatizadas

subsequentes seguirão o padrão de recorrência especificado no campo Schedule expression (Expressão da programação). Se você não marcar a caixa de seleção Enable trigger ao criar a função, poderá editar a função mais tarde para ativar esse acionador.

6. Na página Configurar função, especifique o seguinte:

   - Em Name (Nome), insira um nome para a função.
   - (Opcional) Em Description (Descrição), insira uma descrição que ajudará você a identificar a função mais tarde.
   - Para o tempo de execução, mantenha o valor padrão de**`Node.js 8.10`**. AWS Lambda suporta o inspector-scheduled-runblueprint somente para o **`Node.js 8.10`** tempo de execução.
   - O modelo de avaliação que você deseja executar automaticamente usando essa função. Você faz isso fornecendo o valor para a variável de ambiente chamada assessmentTemplateArn.
   - Mantenha o handler definido como o valor padrão do **`index.handler`**.
   - As permissões para a função usando o campo Função. Para obter mais informações, consulte Modelo de permissões do AWS Lambda.

     Para executar essa função, você precisa de uma função do IAM que permita AWS Lambda iniciar as execuções e gravar mensagens de log sobre as execuções, incluindo quaisquer erros, no Amazon CloudWatch Logs. AWS Lambda assume essa função para cada execução automatizada recorrente. Por exemplo, você pode anexar o seguinte exemplo de política a essa função do IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "inspector:StartAssessmentRun",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

7. Verifique suas seleções e, em seguida, escolha Create function.

Configurar um tópico do SNS para as notificações do Amazon Inspector Classic

O Amazon Simple Notification Service (Amazon SNS) é um serviço da Web que envia mensagens a endpoints ou clientes assinantes do serviço. Você pode usar o Amazon SNS para configurar notificações para o Amazon Inspector Classic.

Para configurar um tópico do SNS para notificações

1. Criar um tópico do SNS. Consulte Tutorial: como criar um tópico do Amazon SNS. Ao criar o tópico, expanda a seção Access policy - optional (Política de acesso – opcional). Em seguida, faça o seguinte para permitir que a avaliação envie mensagens ao tópico:

   a. Em Choose method (Escolher método), selecione Basic (Básico).

   b. Em Definir quem pode publicar mensagens no tópico, escolha Somente as AWS contas especificadas e, em seguida, insira o ARN da conta na região em que você está criando o tópico:

      - `US East (Ohio)` - arn:aws:iam::646659390643:root
      - `US East (N. Virginia)` - arn:aws:iam::316112463485:root
      - `US West (N. California)` - arn:aws:iam::166987590008:root
      - `US West (Oregon)` - arn:aws:iam::758058086616:root
      - `Asia Pacific (Mumbai)` - arn:aws:iam::162588757376:root
      - `Asia Pacific (Seoul)` - arn:aws:iam::526946625049:root
      - `Asia Pacific (Sydney)` - arn:aws:iam::454640832652:root
      - `Asia Pacific (Tokyo)` - arn:aws:iam::406045910587:root
      - `Europe (Frankfurt)` - arn:aws:iam::537503971621:root
      - `Europe (Ireland)` - arn:aws:iam::357557129151:root
      - `Europe (London)` - arn:aws:iam::146838936955:root
      - `Europe (Stockholm)` - arn:aws:iam::453420244670:root
      - `AWS GovCloud (US-East)`- executou: :iam: :206278770380: root aws-us-gov
      - `AWS GovCloud (US-West)`- executou: :iam: :850862329162:root aws-us-gov

c. Em Definir quem pode se inscrever neste tópico, escolha Somente as AWS contas especificadas e, em seguida, insira o ARN da conta na região em que você está criando o tópico.

d. Para se proteger contra o uso do Inspector como substituto confuso, conforme detalhado em Problema do substituto confuso no Guia do Usuário do IAM, faça o seguinte:

i. Escolha Advanced (Avançado). Isso levará você ao editor JSON.

ii. Adicione a seguinte condição:

```
"Condition": {
   "StringEquals": {
     "aws:SourceAccount": <your account Id here>,
     "aws:SourceArn": "arn:aws:inspector:*:*:*"
   }
 }
```

e. (Opcional) Para obter informações adicionais sobre aws: SourceAccount e aws:SourceArn, consulte Chaves de contexto de condição global no Guia do usuário do IAM.

f. Atualize outras configurações para o tópico, conforme necessário, e selecione Create topic (Criar tópico).

2. (Opcional) Para criar um tópico de SNS criptografado, consulte Criptografia em repouso no Guia do desenvolvedor do SNS.

3. Para se proteger contra o Inspector ser usado como um substituto confuso para sua chave KMS, siga as etapas adicionais abaixo:

a. Acesse sua CMK no console KMS.

b. Escolha Editar.

c. Adicione a seguinte condição:

```
"Condition": {
   "StringEquals": {
     "aws:SourceAccount": <your account Id here>,
     "aws:SourceArn": "arn:aws:sns:*:*:*"
   }
 }
```

4. Crie uma inscrição no tópico que você criou. Para obter mais informações, consulte Tutorial: como inscrever um endpoint em um tópico do Amazon SNS.
5. Para verificar se a inscrição está configurada corretamente, publique uma mensagem no tópico. Para obter mais informações, consulte Tutorial: como publicar uma mensagem em um tópico do Amazon SNS.

Descobertas do Amazon Inspector Classic

As descobertas são possíveis problemas de segurança que o Amazon Inspector Classic descobre durante uma avaliação do seu destino de avaliação. As descobertas são exibidas no console do Amazon Inspector Classic ou por meio da API. As descobertas contêm descrições detalhadas dos problemas de segurança e recomendações para resolvê-los.

Uma vez que o Amazon Inspector gera as descobertas, você pode monitorá-las, conferindo atributos específicos do Amazon Inspector Classic a elas. Esses atributos consistem em pares de chave-valor.

Monitorar as descobertas com atributos pode ser útil para gerenciar o fluxo de trabalho de sua estratégia de segurança. Por exemplo, após criar e executar uma avaliação, ela gera uma lista de descobertas com vários graus de severidade, urgência e interesse com base em suas metas e abordagem de segurança. Você pode querer seguir as etapas recomendadas de uma descoberta imediatamente para resolver um possível problema de segurança urgente. Ou talvez você queira adiar a resolução de outra descoberta até a próxima atualização de serviço. Por exemplo, para monitorar uma descoberta e resolver o problema imediatamente, você pode criar e conferir a um atributo a ela com um par de chave-valor de **`Status`** / **`Urgent`**. Você também pode usar atributos para distribuir a carga de trabalho da resolução dos possíveis problemas de segurança. Por exemplo, para oferecer a Pedro (que é um engenheiro de segurança em sua equipe) a tarefa de resolver uma descoberta, você pode conferir a uma descoberta um atributo com um par de chave-valor de **`Assigned Engineer`** / **`Bob`**.

Como trabalhar com descobertas

Conclua o procedimento a seguir gerado em qualquer uma das descobertas do Amazon Inspector Classic.

Para localizar, analisar e conferir atributos à descobertas

1. Faça login AWS Management Console e abra o console do Amazon Inspector Classic em https://console.aws.amazon.com/inspector/.
2. Depois de executar uma avaliação, navegue até a página descobertas no console do Amazon Inspector Classic para exibir as descobertas.

   Você também pode visualizar suas descobertas na seção Descobertas notáveis na página Painel do console do Amazon Inspector Classic.

> **Note**
>
> Não é possível visualizar as descobertas geradas por uma execução de avaliação enquanto ela ainda está em andamento. No entanto, você pode visualizar um subconjunto de descobertas se interromper a avaliação antes que ela conclua sua duração. Em um ambiente de produção, recomendamos que você deixe que cada avaliação seja executada em toda a duração para que ela possa produzir um conjunto completo de descobertas.

3. Para visualizar os detalhes de uma determinada descoberta, selecione o widget Expandir ao lado dessa descoberta. Os detalhes da descoberta incluem o seguinte:

   - O nome do destino de avaliação que inclui a instância do EC2 em que a descoberta foi registrada
   - Nome do modelo de avaliação que foi usado para produzir a descoberta.
   - O horário de início da execução da avaliação.
   - O horário de término da execução da avaliação.
   - O status da execução da avaliação.
   - O nome do pacote de regras que inclui a regra que acionou a descoberta.
   - O nome da descoberta.
   - A severidade da descoberta.
   - Detalhes de severidade nativos do sistema de pontuação de vulnerabilidades comuns (CVSS). Eles incluem indicadores de vetor CVSS e pontuação CVSS (incluindo CVSS versões 2.0 e 3.0) para os resultados acionados pelas regras no pacote de regras de Vulnerabilidades e Exposições comuns. Para obter detalhes sobre o CVSS, consulte https://www.first.org/cvss/.
   - Detalhes de severidade nativos do Center for Internet Security (CIS). Eles incluem a métrica de ponderação do CIS para as descobertas acionadas pelas regras do pacote Referências do CIS. Para obter mais informações sobre métricas de peso do CIS, consulte https://www.cisecurity.org/.
   - A descrição da descoberta.
   - As etapas recomendadas que você pode concluir para corrigir o possível problema de segurança descrito pela descoberta.

4. Para conferir atributos a uma descoberta, escolha a descoberta e, em seguida, escolha Adicionar/editar atributos.

Você também pode conferir atributos a descobertas conforme cria um modelo de avaliação. Para fazer isso, configure o novo modelo para atribuir automaticamente atributos a todas as descobertas geradas pela execução de avaliação. Você pode usar os campos Key (Chave) e Value (Valor) no campo Tags for findings from this assessment (Tags para descobertas desta avaliação). Para ter mais informações, consulte Modelos de avaliação e execuções de avaliação do Amazon Inspector Classic.

5. Para exportar as descobertas para uma planilha, clique no botão de seta para baixo localizado no canto superior direito da página Findings (Descobertas). Na caixa de diálogo, selecione Export all columns (Exportar todas as colunas) ou Export visible columns (Exportar colunas visíveis).

   Observe que no conteúdo exportado, todos os valores de data e hora são timestamps epoch.

6. Para filtrar suas descobertas atuais, insira uma única sequência de caracteres que você quiser filtrar, como uma ID de instância ou número CVE, na barra de filtro acima da tabela de descobertas. Para mostrar ou ocultar colunas de informações adicionais, selecione o ícone de configurações no canto superior direito da página Descobertas.
7. Para excluir as descobertas, navegue até a página Assessment runs (Execuções de avaliação) e selecione a execução que gerou as descobertas que você deseja excluir. Em seguida, selecione Excluir. Quando a confirmação for solicitada, selecione Sim.

   > **Important**
   >
   > Você não pode excluir descobertas individuais no Amazon Inspector Classic. Ao excluir uma execução de avaliação, todas as descobertas e todas as versões do relatório dessa execução também são excluídas.

   Você também pode excluir uma avaliação executada usando a DeleteAssessmentRunAPI.

Relatórios de avaliação

Um relatório de avaliação do Amazon Inspector Classic é um documento que explica o que foi testado em uma execução de avaliação e os resultados da avaliação. Você pode armazenar os relatórios, compartilhá-los com sua equipe para ações de remediação ou acrescentá-los aos dados de auditoria de conformidade. Você pode gerar um relatório para uma execução de avaliação após a conclusão com êxito da execução.

> **Note**
>
> Só é possível gerar relatórios para execuções de avaliação que ocorreram após 25 de abril de 2017, que é a data em que os relatórios de avaliação no Amazon Inspector Classic foram disponibilizados.

Você pode visualizar os seguintes tipos de relatórios de avaliação:

- Relatório de descobertas – esse relatório contém as seguintes informações:
  - Resumo da avaliação
  - As instâncias do EC2 avaliadas durante a execução de avaliação
  - Os pacotes de regras incluídos na execução de avaliação
  - Informações detalhadas sobre cada descoberta, incluindo todas as instâncias do EC2 que tinham a descoberta
- Relatório completo - esse relatório contém todas as informações incluídas em um relatório de descobertas, além de uma lista das regras que foram verificadas em relação às instâncias no destino de avaliação.

Para gerar um relatório de avaliação

1. Na página Assessment runs (Execuções de avaliação), localize a execução de avaliação para a qual você deseja gerar um relatório. Certifique-se de que seu status esteja definido como Analysis complete (Análise completa).
2. Na coluna Reports (Relatórios) dessa execução de avaliação, selecione o ícone de relatórios.

> **Important**
>
> O ícone de relatórios está presente na coluna Reports (Relatórios) somente para as execuções de avaliação que ocorreram ou vão ocorrer após 25 de abril de 2017. Essa é a data em que os relatórios de avaliação foram disponibilizados no Amazon Inspector Classic.

3. Na caixa de diálogo Assessment report (Relatório de avaliação), selecione o tipo de relatório que você deseja visualizar (um relatório de Descobertas ou um relatório Completo) e o formato do relatório (HTML ou PDF). Depois, escolha Generate report (Gerar relatório).

Você também pode gerar relatórios de avaliação por meio da API GetAssessmentReport.

Para excluir um relatório de avaliação, siga o procedimento a seguir.

Para excluir um relatório

- Na página Assessment runs (Execuções de avaliação), selecione a execução em que o relatório que você deseja excluir se baseia e selecione Delete (Excluir). Quando a confirmação for solicitada, selecione Yes (Sim).

  > **Important**
  >
  > No Amazon Inspector Classic, você não conseguirá excluir relatórios individuais. Ao excluir uma execução de avaliação, todas as versões do relatório dessa execução e todas as descobertas também são excluídas.

  Você também pode excluir uma execução de avaliação usando a API DeleteAssessmentRun.

Exclusões no Amazon Inspector Classic

As exclusões são uma saída de execuções de avaliação do Amazon Inspector Classic. As exclusões mostram quais verificações de segurança não podem ser concluídas e como resolver os problemas. Por exemplo, os problemas podem ser causados pela ausência de um agente nas instâncias do EC2 de destino especificadas, pelo uso de um sistema operacional não compatível ou erros inesperados.

Você pode visualizar as exclusões na página Assessment runs (Execuções de avaliação) do console. Para obter mais informações, consulte Como visualizar exclusões pós-avaliação.

Para evitar incorrer em taxas desnecessárias do AWS, o Amazon Inspector Classic permite que você visualize as exclusões antes de executar uma avaliação. Você pode encontrar pré-visualizações na página Assessment templates (Modelos de avaliação) no console. Para obter mais informações, consulte Como visualizar exclusões.

> **Note**
>
> Só é possível gerar exclusões pós-avaliação para as execuções que ocorreram após 25 de junho de 2018. Foi nessa data que as exclusões no Amazon Inspector Classic tornaram-se disponíveis. No entanto, as pré-visualizações de exclusão estão disponíveis para todos os modelos de avaliação, independentemente da data.

Tópicos

Tipos de exclusão

O Amazon Inspector Classic pode produzir os seguintes tipos de exclusão.

Tipo de exclus	Descrição	Recomendação
Nenhu instân na meta	Não há instâncias do EC2 com as tags especificadas no destino de avaliação.	Verifique se as tags em seu destino de avaliação correspondem às tags da instância do EC2 da meta.
O agent já está em execu	Uma execução de avaliação já está em andamento na instância do EC2 da meta.	Aguarde até que a execução de avaliação atual na instância do EC2 da meta seja concluída.
Agent não encon o	Um agente do Amazon Inspector Classic não foi encontrado na instância do EC2 da meta.	Instale ou reinstale o agente do Amazon Inspector Classic na instância do EC2 da meta. Para obter mais

Tipo de exclus	Descrição	Recomendação
		informações, consulte Instalação de agentes do Amazon Inspector Classic.
O agent não é íntegr	O agente do Amazon Inspector Classic na instância do EC2 de destino encontra-se em estado não íntegro.	Verifique o status do agente do Amazon Inspector Classic nesta instância e tome as medidas necessárias. Para obter mais informações, consulte agentes do Inspector.

Tipo de exclus	Descrição	Recomendação
Versã de sisten opera al não compa l	O sistema operacional da instância do EC2 da meta não é compatível com as avaliações do Amazon Inspector Classic.	Remova a instância do EC2 de destino do destino de avaliação ou crie um destino que não inclua essa instância. Para obter uma lista de sistemas operacionais compatíveis, consulte Sistemas operacionais compatíveis com o Amazon Inspector Classic e regiões.

Tipo de exclus	Descrição	Recomendação
Pacot de regras obsole	O modelo de avaliação inclui um pacote de regras obsoleto.	Crie um modelo de avaliação sem o pacote de regras obsoleto e use-o em futuras execuções de avaliação.

Tipo de exclus	Descrição	Recomendação
Pacot de regras não compa l com o sisten opera al	O sistema operacional da instância do EC2 de destino não é compatível com um pacote de regras incluído no modelo de avaliação.	Crie um modelo de avaliação sem os pacotes de regras conflitantes ou remova a instância do EC2 de destino do modelo de avaliação. Para obter uma lista de pacotes de regras comportados por cada sistema operacional, consulte Disponibilidade de pacotes de regras em sistemas operacionais compatíveis.

Tipo de exclus	Descrição	Recomendação
Erro de avalia de regras de uma única instân	Um erro interno provocou uma falha na avaliação de regras para essa instância.	Tente executar a avaliação novamente. Entre em contato com o suporte se a exclusão persistir ao executar novamente a avaliação.
Erro de avalia de regras	Um erro interno provocou uma falha na avaliação de regras de sua avaliação.	Tente executar a avaliação novamente. Entre em contato com o suporte se a exclusão persistir ao executar novamente a avaliação.

Tipo de exclus	Descrição	Recomendação
Erro de acessidade de rede Intern	Um erro interno causou uma falha na avaliação de Acessibilidade de rede durante as verificações de portas acessíveis da Internet. Você pode obter descobertas para outros tipos de Acessibilidade de rede.	Tente executar a avaliação novamente. Entre em contato com o suporte se a exclusão persistir ao executar novamente a avaliação.

Tipo de exclus	Descrição	Recomendação
Erro de Acessidade de rede Intern por meio de um Applic on Load Balan	Um erro interno causou uma falha na avaliação de Acessibilidade de rede durante as verificações de portas acessíveis da Internet por meio de um Application Load Balancer. Você pode obter descobertas para outros tipos de Acessibilidade de rede.	Tente executar a avaliação novamente. Entre em contato com o suporte se a exclusão persistir ao executar novamente a avaliação.

Tipo de exclus	Descrição	Recomendação
Erro de Acessidade de rede Intern por meio de um balanor de carga de elastic ade	Um erro interno causou uma falha na avaliação de Acessibilidade de rede durante as verificações de portas acessíveis da Internet por meio de um balanceador de carga do Balanceador de Carga de Elasticidade. Você pode obter descobertas para outros tipos de Acessibil	Tente executar a avaliação novamente. Entre em contato com o suporte se a exclusão persistir ao executar novamente a avaliação.

Tipo de exclus	Descrição	Recomendação
	idade de rede	
Erro de Acessidade de rede VPN	Um erro interno causou a falha na avaliação de Acessibilidade de rede em verificar a existência de portas acessíveis por VPN. Você pode obter descobertas para outros tipos de Acessibilidade de rede.	Tente executar a avaliação novamente. Entre em contato com o suporte se a exclusão persistir ao executar novamente a avaliação.

Tipo de exclus	Descrição	Recomendação
Erro de Acessidade de rede AWS Direct Conne	Um erro interno causou uma falha na avaliação de Acessibilidade de rede durante as verificações de portas acessíveis por meio do AWS Direct Connect. Você pode obter descobertas para outros tipos de Acessibilidade de rede.	Tente executar a avaliação novamente. Entre em contato com o suporte se a exclusão persistir ao executar novamente a avaliação.

Tipo de exclus	Descrição	Recomendação
Erro de Acessidade de rede empamentc de VPC	Um erro interno causou a falha na avaliação de Acessibilidade de rede em verificar a existência de portas acessíveis por emparelhamento de VPC. Você pode obter descobertas para outros tipos de Acessibilidade de rede.	Tente executar a avaliação novamente. Entre em contato com o suporte se a exclusão persistir ao executar novamente a avaliação.

Como visualizar exclusões

O Amazon Inspector Classic permite que você visualize possíveis exclusões antes de executar uma avaliação.

Para visualizar exclusões de avaliação

1. Faça login no AWS Management Console e abra o console do Amazon Inspector Classic em https://console.aws.amazon.com/inspector/.
2. No painel de navegação, escolha Assessment templates (Modelos de avaliação).
3. Expanda um modelo e, na seção Assessment templates (Modelos de avaliação), selecione Preview exclusions (Visualizar exclusões).
4. Analise as descrições de todas as exclusões detectadas e as recomendações para solucioná-las.

   Você também pode listar e descrever as exclusões usando as operações `ListExclusions` e `DescribeExclusions`.

Como visualizar exclusões pós-avaliação

Depois de executar uma avaliação, você pode visualizar detalhes de qualquer exclusão

Para visualizar detalhes sobre exclusões

1. Faça login no AWS Management Console e abra o console do Amazon Inspector Classic em https://console.aws.amazon.com/inspector/.
2. No painel de navegação, escolha Assessment runs (Execuções de avaliação).
3. Na coluna Exclusions (Exclusões), escolha o link ativo associado à execução de avaliação.
4. Analise as descrições de todas as exclusões detectadas e as recomendações para solucioná-las.

   Você também pode listar e descrever as exclusões usando as operações `ListExclusions` e `DescribeExclusions`.

Pacotes de regras do Amazon Inspector Classic para sistemas operacionais compatíveis

Você pode executar os pacotes de regras do Amazon Inspector Classic nas instâncias do EC2 que estão incluídas em seus destinos de avaliação. A tabela a seguir mostra a disponibilidade dos pacotes de regras para sistemas operacionais compatíveis.

Important

Você pode executar uma avaliação sem agente com o pacote de regras de Acessibilidade de rede em qualquer instância do EC2 independentemente do sistema operacional.

Note

Para obter mais informações sobre os sistemas operacionais compatíveis, consulte Sistemas operacionais e regiões compatíveis com o Amazon Inspector Classic.

Sistemas operacionais compatíveis	Vulnerabilidades e exposições comuns	Referências da CIS	Acessibilidade de rede	Práticas recomendadas de segurança	Análise de comportamento do tempo de execução
Amazon Linux 2	Compatível	Compatível	Compatível	Compatível	Suspenso
Amazon Linux 2018.	Compatível	Compatível	Compatível	Compatível	Suspenso
Amazon Linux 2017.	Compatível	Compatível	Compatível	Compatível	Suspenso

Sistei opera ais comp is	Vulnerabi lidades e exposiçõe s comuns	Referências da CIS	Acessibilidade de rede	Práticas recomendadas de segurança	Análise de comportamento do tempo de execução
Amaz Linux 2017.	Compatíve l	Compatível	Compatível	Compatível	Suspenso
Amaz Linux 2016.	Compatíve l	Compatível	Compatível	Compatível	Suspenso
Amaz Linux 2016.	Compatíve l	Compatível	Compatível	Compatível	Suspenso
Amaz Linux 2015.	Compatíve l	Compatível	Compatível	Compatível	Suspenso
Amaz Linux 2015.	Compatíve l	Compatível	Compatível	Compatível	Suspenso
Amaz Linux 2014.	Compatíve l		Compatível	Compatível	
Amaz Linux 2014.	Compatíve l		Compatível	Compatível	
Amaz Linux 2013.	Compatíve l		Compatível	Compatível	

Sistei operaais compis	Vulnerabilidades e exposições comuns	Referências da CIS	Acessibilidade de rede	Práticas recomendadas de segurança	Análise de comportamento do tempo de execução
Amaz Linux 2013.	Compatível		Compatível	Compatível	
Amaz Linux 2012.	Compatível		Compatível	Compatível	
Amaz Linux 2012.	Compatível		Compatível	Compatível	
Ubun 20.04 LTS	Compatível		Compatível	Compatível	
Ubun 18.04 LTS	Compatível	Compatível	Compatível	Compatível	Suspenso
Ubun 16.04 LTS	Compatível	Compatível	Compatível	Compatível	Suspenso
Ubun 14.04 LTS	Compatível	Compatível	Compatível	Compatível	Suspenso

Sister opera ais comp is	Vulnerabi lidades e exposiçõe s comuns	Referências da CIS	Acessibilidade de rede	Práticas recomendadas de segurança	Análise de comportamento do tempo de execução
Debia 10.x, 9.0 - 9.5, 8.0 - 8.7	Compatíve l		Compatível	Compatível	
RHEL 8.x	Compatíve l		Compatível	Compatível	
RHEL 7.6 - 7.x	Compatíve l	Compatível	Compatível	Compatível	
RHEL 6.2 - 6.9, 7.2 - 7.5	Compatíve l	Compatível	Compatível	Compatível	Suspenso
Cent(7.6 - 7.X	Compatíve l	Compatível	Compatível	Compatível	

Sistei opera ais comp is	Vulnerabi lidades e exposiçõe s comuns	Referências da CIS	Acessibilidade de rede	Práticas recomendadas de segurança	Análise de comportamento do tempo de execução
Cent(6.2 - 6.9, 7.2 - 7.5	Compatíve l	Compatível	Compatível	Compatível	Suspenso
Wind Serve 2019 Base	Compatíve l		Compatível		
Wind Serve 2016 Base	Compatíve l	Compatível	Compatível		Suspenso
Wind Serve 2012 R2	Compatíve l	Compatível	Compatível		Suspenso
Wind Serve 2012	Compatíve l	Compatível	Compatível		Suspenso
Wind Serve 2008 R2	Compatíve l	Compatível	Compatível		Suspenso

Log de chamadas de API da Amazon Inspector Classic com o AWS CloudTrail

O Amazon Inspector Classic está integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, um perfil ou um serviço AWS no Amazon Inspector Classic. O CloudTrail captura todas as chamadas de API para o Amazon Inspector Classic como eventos, inclusive as chamadas do console do Amazon Inspector Classic e de chamadas de código para operações da API do Amazon Inspector Classic. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o Amazon Inspector Classic. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita ao Amazon Inspector Classic, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e outros detalhes.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail. Para obter uma lista completa das operações de API do Amazon Inspector Classic, consulte Ações na Referência de API do Amazon Inspector Classic.

Informações sobre o Amazon Inspector Classic no CloudTrail

O CloudTrail é habilitado em sua conta AWS quando ela é criada. Quando ocorre uma atividade no Amazon Inspector Classic, essa atividade é registrada em um evento do CloudTrail junto com outros eventos de serviços AWS em Histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua conta AWS. Para obter mais informações, consulte Como visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro contínuo de eventos na sua conta AWS, incluindo eventos do Amazon Inspector Classic, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a 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 em log eventos de todas as regiões na partição AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços AWS para analisar mais ainda e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha

- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e Receber arquivos de log do CloudTrail de várias contas

O CloudTrail registra todas as operações do Amazon Inspector Classic, incluindo as operações somente leitura, como `ListAssessmentRuns` e `DescribeAssessmentTargets`, e operações de gerenciamento, como `AddAttributesToFindings` e `CreateAssessmentTemplate`.

> **Note**
>
> O CloudTrail registra somente as informações de solicitação de operações somente leitura do Amazon Inspector Classic. Ambas as informações de solicitação e de resposta são registradas para todas as outras operações do Amazon Inspector Classic.

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 do AWS Identity and Access Management (IAM)
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado
- Se a solicitação foi feita por outro serviço da AWS

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

Noções básicas sobre entradas de arquivos de log do Amazon Inspector Classic

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a ação solicitada, a data e a hora da ação e outros parâmetros de solicitação. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a operação do Amazon Inspector Classic `CreateResourceGroup`:


```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2016-04-14T17:05:54Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2016-04-14T17:12:34Z",
    "eventSource": "inspector.amazonaws.com",
    "eventName": "CreateResourceGroup",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceGroupTags": [
            {
                "key": "Name",
                "value": "ExampleEC2Instance"
            }
        ]
    },
    "responseElements": {
        "resourceGroupArn": "arn:aws:inspector:us-west-2:444455556666:resourcegroup/0-
oclRMp8B"
    },
```

```
    "requestID": "148256d2-0264-11e6-a9b5-b98a7d3b840f",
    "eventID": "e5ea533e-eede-46cc-94f6-0d08e6306ff0",
    "eventType": "AwsApiCall",
    "apiVersion": "v20160216",
    "recipientAccountId": "444455556666"
}
```

Monitorar o Amazon Inspector Classic usando o Amazon CloudWatch

Você pode monitorar o Amazon Inspector Classic usando o Amazon CloudWatch, que coleta e processa dados brutos em métricas legíveis quase que em tempo real. Por padrão, o Amazon Inspector Classic envia dados de métrica ao CloudWatch em períodos de 5 minutos. É possível usar o AWS Management Console, a AWS CLI ou uma API para listar os indicadores que o Amazon Inspector Classic envia para o CloudWatch.

Para obter mais informações sobre o Amazon CloudWatch, consulte o Manual do usuário do Amazon CloudWatch.

Indicadores do Amazon Inspector Classic CloudWatch

O namespace Amazon Inspector Classic no Amazon CloudWatch inclui os indicadores a seguir.

Indicadores da **`AssessmentTargetARN`**:

Indicador	Descrição
`TotalMatchingAgents`	Número de agentes correspondentes a essa meta
`TotalHealthyAgents`	Número de agentes correspondentes a essa meta que estão íntegros
`TotalAssessmentRuns`	Número de execuções de avaliação para essa meta
`TotalAssessmentRun Findings`	Número de descobertas para essa meta

Indicadores da **`AssessmentTemplateARN`**:

Indicador	Descrição
`TotalMatchingAgents`	Número de agentes correspondentes a esse modelo

Indicador	Descrição
`TotalHealthyAgents`	Número de agentes correspondentes a esse modelo que estão íntegros
`TotalAssessmentRuns`	Número de execuções de avaliação para esse modelo
`TotalAssessmentRun Findings`	Número de descobertas para esse modelo

Indicadores agregados

Indicador	Descrição
`TotalAssessmentRuns`	Número de execuções de avaliação nessa conta AWS

Configurando o Amazon Inspector Classic usando AWS CloudFormation

Para obter informações de referência sobre os recursos do Amazon Inspector Classic que são compatíveis com AWS CloudFormation, consulte os seguintes tópicos:

- `AWS::Inspector::AssessmentTarget`
- `AWS::Inspector::AssessmentTemplate`
- `AWS::Inspector::ResourceGroup`

> **Important**
>
> Para obter listas dos ARNs dos pacotes de regras do Amazon Inspector Classic em regiões da AWS compatíveis, consulte Amazon Inspector Classic ARNS para pacotes de regras.

Integração com o AWS Security Hub

O AWS Security Hub fornece uma visão abrangente do estado de segurança na AWS e ajuda a verificar o ambiente em relação aos padrões e às práticas recomendadas do setor de segurança. O Security Hub coleta dados de segurança de contas, serviços e produtos compatíveis de terceiros parceiros da AWS e ajuda a analisar suas tendências de segurança e identificar os problemas de segurança de prioridade mais alta.

A integração do Amazon Inspector com o Security Hub permite que você envie descobertas do Amazon Inspector para o Security Hub. O Security Hub pode então incluir tais descobertas na análise feita sobre a seu procedimento de segurança.

Sumário

Como o Amazon Inspector envia as descobertas para o Security Hub

No Security Hub, os problemas de segurança são rastreados como descobertas. Algumas descobertas provêm de problemas que são detectados por outros produtos da AWS ou por parceiros terceirizados. O Security Hub também tem um conjunto de regras que ele usa para detectar problemas de segurança e gerar descobertas.

O Security Hub fornece ferramentas para gerenciar descobertas em todas essas fontes. Você pode exibir e filtrar listas de descobertas e exibir detalhes de uma descoberta. Consulte Visualizar 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 – Formato de Descoberta de Segurança da AWS). O ASFF inclui detalhes sobre a origem do problema, os recursos afetados e o status atual da descoberta. Consulte o Security Finding Format (ASFF) no Guia do usuário do AWS Security Hub.

O Amazon Inspector é um dos serviços AWS que envia descobertas para o Security Hub.

Tipos de descobertas que o Amazon Inspector envia

O Amazon Inspector envia todas as descobertas que gera para o Security Hub.

O Amazon Inspector envia descobertas para o Security Hub usando o AWS Security Finding Format (ASFF). No ASFF, o campo `Types` fornece o tipo de descoberta. As descobertas do Amazon Inspector podem ter os seguintes valores para `Types`.

- Verificações de software e configuração/vulnerabilidades/CVE
- Verificações de software e configuração/práticas recomendadas de segurança da AWS/ Acessibilidade de rede
- Verificações de software e configuração/padrões setoriais e regulatórios/benchmarks do CIS Host Hardening

Latência para enviar descobertas

Quando o Amazon Inspector cria uma nova descoberta, ela geralmente é enviada para o Security Hub em cinco minutos.

Tentar novamente quando o Security Hub não estiver disponível

Se o Security Hub não estiver disponível, o Amazon Inspector tentará enviar novamente as descobertas até que sejam recebidas.

Atualizar as descobertas existentes no Security Hub

Depois de enviar uma descoberta ao Security Hub, o Amazon Inspector atualiza a descoberta para refletir observações adicionais da atividade de descoberta. Isso resultará em menos descobertas do Amazon Inspector no Security Hub do que no Amazon Inspector.

Descoberta típica do Amazon Inspector

O Amazon Inspector envia descobertas para o Security Hub usando o AWS Security Finding Format (ASFF).

Aqui está um exemplo de uma descoberta típica do Amazon Inspector.


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
  "GeneratorId": "arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd",
  "AwsAccountId": "111122223333",
  "Types": [
    "Software and Configuration Checks/AWS Security Best Practices/Network Reachability
 - Recognized port reachable from internet"
  ],
  "CreatedAt": "2020-08-19T17:36:22.169Z",
  "UpdatedAt": "2020-11-04T16:36:06.064Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "6.0"
  },
  "Confidence": 10,
  "Title": "On instance i-0c10c2c7863d1a356, TCP port 22 which is associated with 'SSH'
is reachable from the internet",
  "Description": "On this instance, TCP port 22, which is associated with SSH, is
reachable from the internet. You can install the Inspector agent on this instance
and re-run the assessment to check for any process listening on this port. The
instance i-0c10c2c7863d1a356 is located in VPC vpc-a0c2d7c7 and has an attached ENI
eni-078eac9d6ad9b20d1 which uses network ACL acl-154b8273. The port is reachable from
the internet through Security Group sg-0af64c8a5eb30ca75 and IGW igw-e209d785",
  "Remediation": {
    "Recommendation": {
      "Text": "You can edit the Security Group sg-0af64c8a5eb30ca75 to remove access
from the internet on port 22"
    }
  },
  "ProductFields": {
    "attributes/VPC": "vpc-a0c2d7c7",
    "aws/inspector/id": "Recognized port reachable from internet",
```

```
    "serviceAttributes/schemaVersion": "1",
    "aws/inspector/arn": "arn:aws:inspector:us-east-1:111122223333:target/0-8zh1cWkg/
template/0-rqtRV0u0/run/0-Ck2F6tY9/finding/0-B458MQWe",
    "attributes/ACL": "acl-154b8273",
    "serviceAttributes/assessmentRunArn": "arn:aws:inspector:us-
east-1:111122223333:target/0-8zh1cWkg/template/0-rqtRV0u0/run/0-Ck2F6tY9",
    "attributes/PROTOCOL": "TCP",
    "attributes/RULE_TYPE": "RecognizedPortNoAgent",
    "aws/inspector/RulesPackageName": "Network Reachability",
    "attributes/INSTANCE_ID": "i-0c10c2c7863d1a356",
    "attributes/PORT_GROUP_NAME": "SSH",
    "attributes/IGW": "igw-e209d785",
    "serviceAttributes/rulesPackageArn": "arn:aws:inspector:us-
east-1:111122223333:rulespackage/0-PmNV0Tcd",
    "attributes/SECURITY_GROUP": "sg-0af64c8a5eb30ca75",
    "attributes/ENI": "eni-078eac9d6ad9b20d1",
    "attributes/REACHABILITY_TYPE": "Internet",
    "attributes/PORT": "22",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/inspector/
inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
    "aws/securityhub/ProductName": "Inspector",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475"
        }
      }
    }
  ],
```

```
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```

Habilitar e configurar a integração

Para usar a integração com o Security Hub, você deve habilitar o Security Hub. Para obter informações sobre como habilitar o Security Hub, consulte Configurar o Security Hub no Guia do usuário AWS Security Hub.

Ao habilitar tanto o Amazon Inspector e o Security Hub, a integração é habilitada automaticamente. O Amazon Inspector começa a enviar descobertas para o Security Hub.

Como parar de enviar descobertas

Para parar de enviar descobertas para o Security Hub, você pode usar o console do Security Hub ou o API.

Consulte Desabilitar e habilitar o fluxo de descobertas de uma integração (console) ou Desabilitar o fluxo de descobertas de uma integração (API do Security Hub, AWA CLI) no Guia do usuário do AWS Security Hub.

Amazon Inspector Classic ARNs

Cada tipo de pacote de regras e recursos no Amazon Inspector Classic tem um nome do recurso da Amazon (ARN) exclusivo associado a ele.

Sumário

ARNs para recursos do Amazon Inspector Classic

No Amazon Inspector Classic, os principais recursos são grupos de recursos, destinos de avaliação, modelos de avaliação, execuções de avaliação e descobertas. Esses recursos têm nomes dos recursos da Amazon exclusivos associados, conforme mostrado na tabela a seguir.

Tipo de recurso	Formato de nome do recurso da Amazon (ARN)
Grupo de recursos	`arn:aws:inspector:` *region*`:`*account-id* `:resourcegroup/` *ID*
destino de avaliação	`arn:aws:inspector:` *region*`:`*account-id* `:target/`*ID*
Modelo de avaliação	`arn:aws:inspector:` *region*`:`*account-id* `:target/`*ID*`:template:` *ID*
Execução de avaliação	`arn:aws:inspector:` *region*`:`*account-id* `:target/`*ID*`/template/` *ID*`/run/`*ID*
Descoberta	`arn:aws:inspector:` *region*`:`*account-id* `:target/`*ID*`/template/` *ID*`/run/`*ID*`/finding/` *ID*

Amazon Inspector Classic ARNS para pacotes de regras

As tabelas abaixo mostram os ARNs para pacotes de regras do Amazon Inspector Classic em todas as regiões suportadas.

Tópicos

- AWS GovCloud (Leste dos EUA)
- AWS GovCloud (Oeste dos EUA)

Leste dos EUA (Ohio)

Nome do pacote de regras	ARN
Vulnerabilidades e exposições comuns	`arn:aws:inspector:us-east-2:646659390643:rulespackage/0-JnA8Zp85`
Referências de configuração de segurança do sistema operacional CIS	`arn:aws:inspector:us-east-2:646659390643:rulespackage/0-m8r61nnh`
Acessibilidade de rede	`arn:aws:inspector:us-east-2:646659390643:rulespackage/0-cE4kTR30`
Práticas recomendadas de segurança	`arn:aws:inspector:us-east-2:646659390643:rulespackage/0-AxKmMHPX`

Leste dos EUA (N. da Virgínia)

Nome do pacote de regras	ARN
Vulnerabilidades e exposições comuns	`arn:aws:inspector:us-east-1:316112463485:rulespackage/0-gEjTy7T7`

Nome do pacote de regras	ARN
Referências de configuração de segurança do sistema operacional CIS	`arn:aws:inspector:us-east-1:316112463485:rulespackage/0-rExsr2X8`
Acessibilidade de rede	`arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd`
Práticas recomendadas de segurança	`arn:aws:inspector:us-east-1:316112463485:rulespackage/0-R01qwB5Q`

Oeste dos EUA (N. da Califórnia)

Nome do pacote de regras	ARN
Vulnerabilidades e exposições comuns	`arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TKgzoVOa`
Referências de configuração de segurança do sistema operacional CIS	`arn:aws:inspector:us-west-1:166987590008:rulespackage/0-xUY8iRqX`
Acessibilidade de rede	`arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TxmXimXF`

Nome do pacote de regras	ARN
Práticas recomendadas de segurança	`arn:aws:inspector:us-west-1:166987590008:rulespackage/0-byoQRFYm`

Oeste dos EUA (Oregon)

Nome do pacote de regras	ARN
Vulnerabilidades e exposições comuns	`arn:aws:inspector:us-west-2:758058086616:rulespackage/0-9hgA516p`
Referências de configuração de segurança do sistema operacional CIS	`arn:aws:inspector:us-west-2:758058086616:rulespackage/0-H5hpSawc`
Acessibilidade de rede	`arn:aws:inspector:us-west-2:758058086616:rulespackage/0-rD1z6dpl`
Práticas recomendadas de segurança	`arn:aws:inspector:us-west-2:758058086616:rulespackage/0-JJOtZiqQ`

Ásia-Pacífico (Mumbai)

Nome do pacote de regras	ARN
Vulnerabilidades e exposições comuns	`arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-LqnJE9dO`
Referências de configuração de segurança do sistema operacional CIS	`arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-PSUlX14m`
Acessibilidade de rede	`arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-YxKfjFu1`
Práticas recomendadas de segurança	`arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-fs0IZZBj`

Ásia-Pacífico (Seul)

Nome do pacote de regras	ARN
Vulnerabilidades e exposições comuns	`arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-PoGHMznc`
Referências de configuração de segurança do sistema operacional CIS	`arn:aws:inspector:ap-northeast-2:526`

Nome do pacote de regras	ARN
	946625049:rulespac kage/0-T9srhg1z
Acessibilidade de rede	arn:aws:inspector: ap-northeast-2:526 946625049:rulespac kage/0-s3OmLzhL
Práticas recomendadas de segurança	arn:aws:inspector: ap-northeast-2:526 946625049:rulespac kage/0-2WRpmi4n

Ásia-Pacífico (Sydney)

Nome do pacote de regras	ARN
Vulnerabilidades e exposições comuns	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-D5TGAxiR
Referências de configuração de segurança do sistema operacional CIS	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-Vkd2Vxjq
Acessibilidade de rede	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-FLcuV4Gz
Práticas recomendadas de segurança	arn:aws:inspector: ap-southeast-2:454

Nome do pacote de regras	ARN
	640832652:rulespac kage/0-asL6HRgN

Ásia-Pacífico (Tóquio)

Nome do pacote de regras	ARN
Vulnerabilidades e exposições comuns	arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-gHP9oWNT
Referências de configuração de segurança do sistema operacional CIS	arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-7WNjqgGu
Acessibilidade de rede	arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-YI95DVd7
Práticas recomendadas de segurança	arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-bBUQnxMq

Europa (Frankfurt)

Nome do pacote de regras	ARN
Vulnerabilidades e exposições comuns	arn:aws:inspector: eu-central-1:53750

Nome do pacote de regras	ARN
	3971621:rulespackage/0-wNqHa8M9
Referências de configuração de segurança do sistema operacional CIS	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-nZrAVuv8
Acessibilidade de rede	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-6yunpJ91
Práticas recomendadas de segurança	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-ZujVHEPB

Europa (Irlanda)

Nome do pacote de regras	ARN
Vulnerabilidades e exposições comuns	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-ubA5XvBh
Referências de configuração de segurança do sistema operacional CIS	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-sJBhCr0F
Acessibilidade de rede	arn:aws:inspector:eu-west-1:35755712

Nome do pacote de regras	ARN
	9151:rulespackage/0-SPzU33xe
Práticas recomendadas de segurança	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-SnojL3Z6

Europa (Londres)

Nome do pacote de regras	ARN
Vulnerabilidades e exposições comuns	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-kZGCqcE1
Referências de configuração de segurança do sistema operacional CIS	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-IeCjwf1W
Acessibilidade de rede	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-AizSYyNq
Práticas recomendadas de segurança	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-XApUiSaP

Europa (Estocolmo)

Nome do pacote de regras	ARN
Vulnerabilidades e exposições comuns	`arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-IgdgIewd`
Referências de configuração de segurança do sistema operacional CIS	`arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-Yn8jlX7f`
Acessibilidade de rede	`arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-52Sn74uu`
Práticas recomendadas de segurança	`arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-HfBQSbSf`

AWS GovCloud (Leste dos EUA)

Nome do pacote de regras	ARN
Vulnerabilidades e exposições comuns	`arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-3IFKFu0b`
Referências de configuração de segurança do sistema operacional CIS	`arn:aws-us-gov:inspector:us-gov-east`

Nome do pacote de regras	ARN
	-1:206278770380:rulespackage/0-pTLCdIww
Práticas recomendadas de segurança	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-vlgEGcVD

AWS GovCloud (Oeste dos EUA)

Nome do pacote de regras	ARN
Vulnerabilidades e exposições comuns	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-4oQgcI4G
Referências de configuração de segurança do sistema operacional CIS	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-Ac4CFOuc
Práticas recomendadas de segurança	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-rOTGqe5G

Histórico do documento

A tabela a seguir descreve o histórico de versões da documentação do Amazon Inspector Classic posterior a maio de 2018.

Alteração	Descrição	Data
Práticas recomendadas de segurança atualizadas para senhas	Os requisitos de práticas recomendadas de segurança do Amazon Inspector Classic para o tamanho da senha da instância do EC2 e a complexidade da senha foram atualizados. Consulte Configurar o tamanho mínimo da senha e Configurar a complexidade da senha	8 de março de 2021
Suporte adicionado para versões mais recentes do sistema operacional	O Amazon Inspector Classic agora suporta as seguintes versões do sistema operacional: Ubuntu 20.4 LTS, Debian 10.x, RHEL 8.x, e Windows Server 2019 Base.	15 de outubro de 2020
Informações de segurança consolidadas em um novo capítulo de segurança	As informações de segurança do Amazon Inspector Classic, incluindo informações sobre gerenciamento de identidades e gerenciamento de acesso, são consolidadas em um capítulo de segurança. Consulte Segurança no Amazon Inspector Classic.	7 de abril de 2020
Documentação atualizada para remover o suporte ao	Vários tópicos foram atualizados para remover informações	5 de setembro de 2019

pacote de regras de análise de comportamento do tempo de execução.	sobre o pacote de regras de análise de comportamento do tempo de execução, que não é mais compatível.	
Suporte adicionado para sistema operacional	Foi adicionado suporte ao Amazon Inspector Classic para CentOS 7.6. Para obter mais informações, consulte Regiões e sistemas operacionais compatíveis com o Amazon Inspector Classic e Disponibilidade de pacotes de regras em sistemas operacionais compatíveis.	3 de dezembro de 2018
Novo conteúdo	Adição do pacote de regras de Acessibilidade de rede do Amazon Inspector Classic, que permite que os usuários executem avaliações de configuração de rede sem agentes para as vulnerabilidades de segurança. Para obter mais informações, consulte Acessibilidade de rede.	9 de novembro de 2018

Suporte adicionado para sistema operacional	Suporte do Amazon Inspector Classic adicionado para o RHEL 7.6. Para obter mais informações, consulte Regiões e sistemas operacionais compatíveis com o Amazon Inspector Classic e Disponibilidade de pacotes de regras em sistemas operacionais compatíveis.	30 de outubro de 2018
Suporte adicionado para sistema operacional	Adicionado suporte para diversos sistemas operacionais para os pacotes de regras de referência da CIS. Para mais informações, consulte Referências da central de segurança da internet (CIS) e Disponibilidade de pacotes de regras em sistemas operacionais compatíveis.	13 de agosto de 2018
Adição de suporte para a região	Adição de suporte por região para `AWS GovCloud (US)`	13 de junho de 2018

A tabela abaixo descreve o histórico de versões da documentação do Amazon Inspector Classic antes de junho de 2018.

Alteração	Descrição	Data
Novo conteúdo	Capacidade adicionada para atender a todas as instâncias do Amazon EC2 em uma conta. Para ter mais informações, consulte	24 de maio de 2018

Alteração	Descrição	Data
	Destinos de avaliação do Amazon Inspector Classic.	
Suporte adicionado para sistema operacional	Foi adicionado suporte ao Amazon Inspector Classic para Amazon Linux 2018.03 e Ubuntu 18.04.	15 de maio de 2018
Novo conteúdo	Capacidade adicionada para configurar avaliaçõe s recorrentes do Amazon Inspector Classic.	30 de abril de 2018
Novo conteúdo	Capacidade adicionada para instalar um agente do Amazon Inspector Classic por meio do console.	30 de abril de 2018
Suporte adicionado para sistema operacional	Adicionado suporte para o Amazon Inspector Classic para o Amazon Linux 2.	13 de março de 2018
Suporte adicionado para sistema operacional	Suporte de avaliação do Amazon Inspector Classic adicionado para Windows Server 2016 Base.	20 de fevereiro de 2018
Adição de suporte para a região	Foi adicionado suporte ao Amazon Inspector Classic para a região `US East (Ohio)`.	7 de fevereiro de 2018
Novo conteúdo	Agora as avaliações do Amazon Inspector Classic podem ser executadas quando o módulo do kernel está indisponível.	11 de janeiro de 2018

Alteração	Descrição	Data
Adição de suporte para a região	Foi adicionado suporte ao Amazon Inspector Classic para a região `EU (Frankfurt)` .	19 de dezembro de 2017
Novo conteúdo	Capacidade adicionada para verificar a integridade do agente doAPI e console do Amazon Inspector Classic.	15 de dezembro de 2017
Novo conteúdo	Os seguintes recursos foram adicionados: • Uso de função vinculada ao serviço • AMI do agente Amazon Inspector Classic disponível no Marketplace AWS • Modelos do Amazon Inspector Classic AWS CloudFormation	5 de dezembro de 2017
Suporte adicionado para sistema operacional	Suporte de avaliação do Amazon Inspector Classic adicionado para o CentOS 7.4.	9 de novembro de 2017
Suporte adicionado para sistema operacional	Suporte de avaliação do Amazon Inspector Classic adicionado para o Amazon Linux 2017.09.	11 de outubro de 2017
Suporte adicionado para sistema operacional	Suporte de avaliação do Amazon Inspector Classic adicionado para o RHEL 7.4.	20 de fevereiro de 2018

Alteração	Descrição	Data
Qualificação pela HIPAA adicionada	O Amazon Inspector Classic agora está qualificado para a HIPAA.	31 de julho de 2017
Novo conteúdo	Foi adicionada a capacidade de acionar automaticamente a avaliação de segurança do Amazon Inspector Classic com o Amazon CloudWatch Events.	27 de julho de 2017
Adição de suporte para a região	Foi adicionado suporte ao Amazon Inspector Classic para a região `US West (N. California)` .	6 de junho de 2018
Suporte adicionado para sistema operacional	Suporte de avaliação do Amazon Inspector Classic adicionado para RHEL 6.2-6.9, RHEL 7.2-7.3, CentOS 6.9 e CentOS 7.2-7.3.	23 de maio de 2017
Suporte adicionado para sistema operacional	Suporte de avaliação do Amazon Inspector Classic adicionado para o Amazon Linux 2017.03.	25 de abril de 2017
Novo conteúdo e suporte adicionado para sistema operacional	O que foi adicionado: • Suporte do Amazon Inspector Classic para o Ubuntu 16.04. • Disponibilidade do esquema Lambda para automatizar as operações do Amazon Inspector Classic.	5 de janeiro de 2017

Alteração	Descrição	Data
Novo suporte para sistema operacional	Suporte do Amazon Inspector Classic adicionado para o Microsoft Windows.	26 de agosto de 2016
Adição de suporte para a região	Foi adicionado suporte ao Amazon Inspector Classic para a região `Asia Pacific (Seoul)`.	26 de agosto de 2016
Adição de suporte para a região	Foi adicionado suporte ao Amazon Inspector Classic para a região `Asia Pacific (Mumbai)`.	25 de abril de 2016
Adição de suporte para a região	Foi adicionado suporte ao Amazon Inspector Classic para a região `Asia Pacific (Sydney)`.	25 de abril de 2016
Inicialização do serviço	Lançamento dos serviços Amazon Inspector Classic.	7 de outubro de 2015

Glossário do AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.