Manual do usuário

AWS Security Hub

AWS Security Hub: Manual do usuário

Table of Contents

O que é o AWS Security Hub?

O AWS Security Hub fornece a você uma visão abrangente do seu estado de segurança na AWS e ajuda a avaliar o seu ambiente AWS de acordo com os padrões e as melhores práticas do setor de segurança.

O Security Hub coleta dados de segurança das Contas da AWS, Serviços da AWS e produtos de parceiros compatíveis, além de ajudar a analisar suas tendências de segurança e identificar os problemas de segurança de prioridade mais alta.

Para ajudar você a gerenciar o estado de segurança da sua organização, o Security Hub é compatível com vários padrões de segurança. Isso inclui o padrão Práticas Recomendadas de Segurança Básica (FSBP) da AWS, desenvolvido pela AWS, e estruturas externas de conformidade, como o Center for Internet Security (CIS — Centro de segurança na Internet), o Payment Card Industry Data Security Standard (PCI DSS — Padrão de segurança de dados do setor de cartões de pagamento) e o National Institute of Standards and Technology (NIST — Instituto nacional de padrões e tecnologia). Cada padrão inclui vários controles de segurança, cada um dos quais representa uma prática recomendada de segurança. O Security Hub executa verificações nos controles de segurança e gera descobertas de controle para ajudar você a avaliar sua conformidade com as melhores práticas de segurança.

Além de gerar descobertas de controle, o Security Hub também recebe descobertas de outros, Serviços da AWS como Amazon GuardDuty, Amazon Inspector e Amazon Macie, e de produtos de terceiros compatíveis. Isso fornece um único painel de controle sobre uma variedade de problemas relacionados à segurança. Você também pode enviar as descobertas do Security Hub para outros Serviços da AWS e produtos de terceiros compatíveis.

O Security Hub oferece atributos de automação que ajudam você a fazer a triagem e corrigir problemas de segurança. Por exemplo, é possível usar regras de automação para atualizar automaticamente descobertas críticas quando uma verificação de segurança falha. Você também pode aproveitar a integração com a Amazon EventBridge para acionar respostas automáticas a descobertas específicas.

Tópicos

- Avaliação gratuita e preços do Security Hub

Benefícios do Security Hub

Aqui estão algumas das principais maneiras pelas quais o Security Hub ajuda você a monitorar sua postura de conformidade e segurança em todo o seu ambiente AWS.

Esforço reduzido para coletar e priorizar descobertas

O Security Hub reduz a tentativa de coletar e priorizar as descobertas de segurança nas contas de Serviços da AWS integrados e de produtos de parceiros da AWS. O Security Hub processa a descoberta de dados usando o AWS Formato do Security Finding (ASFF), um formato de descoberta padrão. Isso elimina a necessidade de gerenciar descobertas de inúmeras fontes em vários formatos. Depois, o Security Hub correlaciona as descobertas dos provedores para priorizar as mais importantes.

Verificações automáticas de segurança em relação aos padrões e às melhores práticas

O Security Hub executa automaticamente verificações de segurança e de configuração contínuas no nível de conta com base nas melhores práticas da AWS e nos padrões do setor. O Security Hub usa os resultados dessas verificações para calcular as pontuações de segurança e identifica contas e recursos específicos que exigem atenção.

Visualização consolidada das descobertas nas contas e nos provedores

O Security Hub consolida suas descobertas de segurança em contas e em produtos do provedor e exibe os resultados no console do Security Hub. Você também pode recuperar descobertas por meio da API do Security Hub, do AWS CLI ou dos SDKs. Com uma visão ampla do seu status de segurança atual, é possível detectar tendências, identificar possíveis problemas e tomar as medidas de correção necessárias.

Capacidade de automatizar a correção e atualização de descobertas

É possível criar regras de automação que modificam ou suprimem descobertas com base nos critérios definidos. O Security Hub também oferece suporte à integração com a Amazon EventBridge. Para automatizar a correção de descobertas específicas, é possível definir ações personalizadas a serem executadas quando uma descoberta é recebida. Por exemplo, é possível configurar ações personalizadas para enviar as descobertas a um sistema de criação de tíquetes ou a um sistema automatizado de correção.

Acessando o Security Hub

O Security Hub está disponível na maioria das Regiões da AWS. Para obter uma lista de todas as regiões onde o Security Hub está disponível no momento, consulte AWS Endpoints e cotas do Security Hub no Referência geral da AWS. Para obter informações sobre como gerenciar as Regiões da AWS em sua Conta da AWS, consulte Especificação de qual Regiões da AWS sua conta pode usar no Guia de referência do AWS Account Management.

Em cada região, é possível acessar e usar o Security Hub de qualquer uma das maneiras a seguir:

Console do Security Hub

O AWS Management Console é uma interface baseada em navegador que pode ser usada para criar e gerenciar recursos da AWS. Como parte desse console, o console do Security Hub fornece acesso à sua conta, dados e recursos do Security Hub. É possível realizar tarefas do Security Hub usando o console do Security Hub: visualize descobertas, crie regras de automação, crie uma região de agregação e muito mais.

API do Security Hub

A API do Security Hub oferece acesso programático à sua conta, dados e recursos do Security Hub. Com a API, é possível enviar solicitações HTTPS diretamente para o Security Hub. Para mais informações sobre a API, consulte a Referência de API do AWS Security Hub.

AWS CLI

Com o AWS CLI, é possível executar comandos na linha de comando do seu sistema e realizar tarefas com o Security Hub. Em alguns casos, usar a linha de comando pode ser mais rápido e mais conveniente do que usar o console. A linha de comando também é útil se você quiser criar scripts que realizem tarefas. Para obter informações sobre a instalação e o uso da AWS CLI, consulte o Guia do usuário da AWS Command Line Interface.

SDKs da AWS

A AWS fornece SDKs que consistem em bibliotecas e códigos de exemplo para várias linguagens de programação e plataformas, como Java, Go, Python, C++ e .NET. Os SDKs fornecem acesso conveniente e programático ao Security Hub e outros Serviços da AWS no idioma de sua preferência. Também incluem tarefas como assinatura criptográfica de solicitações, gerenciamento de erros e novas tentativas automáticas de solicitações. Para informações sobre como instalar e usar os SDKs da AWS, consulte Ferramentas para criar na AWS.

> **Important**
>
> O Security Hub só detecta e consolida descobertas geradas após a habilitação do Security Hub. Ele não detecta e consolida retroativamente descobertas de segurança que foram geradas antes da habilitação do Security Hub.
> O Security Hub só recebe e processa as descobertas da região em que você habilitou o Security Hub em sua conta.
> Para total conformidade com as verificações de segurança do CIS AWS Foundations Benchmark, é necessário habilitar o Security Hub em todas as regiões da AWS compatíveis.

Serviços relacionados

Para proteger ainda mais seu ambiente AWS, considere usar outro Serviços da AWS em combinação com o Security Hub.

Para obter uma lista de outros Serviços da AWS que enviam ou recebem descobertas do Security Hub, consulte AWS service (Serviço da AWS) integrações com o AWS Security Hub.

O Security Hub usa regras vinculadas a serviços do AWS Config para executar verificações de segurança na maioria dos controles. Você deve habilitar o AWS Config e registrar recursos no AWS Config para o Security Hub para gerar a maioria das descobertas de controle. Para ter mais informações, consulte Configurando AWS Config.

Avaliação gratuita e preços do Security Hub

Ao habilitar o Security Hub em uma Conta da AWS pela primeira vez, essa conta será inscrita automaticamente em uma avaliação gratuita de 30 dias do Security Hub.

Quando você usa o Security Hub durante a avaliação gratuita, precisa pagar pelo uso de outros serviços com os quais o Security Hub interage, como itens do AWS Config. Você não é cobrado por regras do AWS Config ativadas somente pelos padrões de segurança do Security Hub.

Você não será cobrado por usar o Security Hub até o término da avaliação gratuita.

> **Note**
>
> A avaliação gratuita do Security Hub não é compatível na região da China (Pequim).

Visualizar detalhes de uso e custo estimado

O Security Hub fornece informações de uso, incluindo um custo estimado de 30 dias pelo uso do Security Hub. Os detalhes de uso incluem o tempo restante da avaliação gratuita. As informações de uso podem ajudar você a entender quais podem ser os custos do Security Hub após o término da avaliação gratuita. As informações de uso também estão disponíveis após o término da avaliação gratuita.

Para exibir informações de uso (console)

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Uso em Configurações.

O custo mensal estimado é baseado no uso da sua conta do Security Hub para descobertas e verificações de segurança projetadas em um período de 30 dias.

As informações de uso e o custo estimado são somente para a conta corrente e a região atual. Em uma região de agregação, as informações de uso e o custo estimado não incluem regiões vinculadas. Para mais informações sobre regiões, consulte the section called “Como funciona a agregação entre regiões”.

Detalhes de preço

Para mais informações sobre como o Security Hub cobra por descobertas de ingestão e verificações de segurança, consulte a Definição de preços do Security Hub.

Conceitos do Security Hub

Este tópico descreve os principais conceitos e terminologia do AWS Security Hub para ajudar você a começar a usar o serviço.

Conta

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

Uma conta pode convidar outras contas para habilitar o Security Hub e se associar a essa conta no Security Hub. Aceitar um convite de associação é opcional. Se os convites forem aceitos, a conta se torna uma conta de administrador e as contas adicionadas serão contas-membro. As contas de administrador podem ver as descobertas em suas contas-membro.

Se você estiver inscrito AWS Organizations, sua organização designará uma conta de administrador do Security Hub para a organização. A conta de administrador do Security Hub pode habilitar outras contas da organização como contas-membro.

Uma conta não pode ser uma conta de administrador e uma conta-membro ao mesmo tempo. Uma conta só pode ter uma conta de administrador.

Para ter mais informações, consulte Gerenciar contas de administrador e membro.

Conta de administrador

Uma conta no Security Hub com acesso para visualizar as descobertas das contas-membro associadas.

Uma conta se torna uma conta de administrador de uma das seguintes maneiras:

- A conta convida outras contas a se associarem a ela no Security Hub. Quando essas contas aceitam o convite, elas se tornam contas-membro e a conta que enviou o convite se torna sua conta de administrador.
- A conta é designada por uma conta de gerenciamento da organização como a conta de administrador do Security Hub. A conta de administrador do Security Hub pode habilitar qualquer conta da organização como uma conta-membro e pode convidar outras contas para serem contas-membro.

Uma conta só pode ter uma conta de administrador. Uma conta não pode ser uma conta de administrador e uma conta-membro ao mesmo tempo.

Região de agregação

Definir uma região de agregação permite que você visualize as descobertas de segurança de várias Regiões da AWS em um único painel de vidro.

A região de agregação é a região a partir da qual você visualiza e gerencia as descobertas. As descobertas são agregadas à região de agregação das regiões vinculadas. As atualizações das descobertas são replicadas em todas as regiões.

Na região de agregação, as páginas Padrões de segurança, Insights e Descobertas incluem dados de todas as regiões vinculadas.

Consulte Agregação entre regiões.

Descoberta arquivada

Uma descoberta que tem um `RecordState` definido como `ARCHIVED`. O arquivamento de uma descoberta indica que o provedor da descoberta acredita que ela não é mais relevante. O estado do registro é separado do status do fluxo de trabalho, que rastreia o status de uma investigação em uma descoberta.

Os provedores de descobertas podem usar a operação `BatchImportFindings` da API do Security Hub para arquivar as descobertas que eles criaram. O Security Hub arquivará automaticamente descobertas de controles se o controle for desabilitado ou se o recurso associado for excluído, com base em um dos critérios a seguir.

- A descoberta não é atualizada em três a cinco dias (observe que esse é a melhor tentativa e não é garantida).
- A AWS Config avaliação associada retorna`NOT_APPLICABLE`.

Por padrão, as descobertas arquivadas são excluídas das listas de descobertas no console do Security Hub. É possível atualizar o filtro para incluir descobertas arquivadas.

A operação `GetFindings` da API do Security Hub retorna tanto descobertas ativas como arquivadas. Você pode incluir um filtro para o estado do registro.

```
"RecordState": [
    {
        "Comparison": "EQUALS",
        "Value": "ARCHIVED"
    }
```

```
],
```

AWS Formato de descoberta de segurança (ASFF)

Um formato padronizado para o conteúdo de descobertas que o Security Hub agrega ou gera. O Formato de descoberta de AWS segurança permite que você use o Security Hub para visualizar e analisar descobertas geradas por serviços de AWS segurança, soluções de terceiros ou pelo próprio Security Hub a partir da execução de verificações de segurança. Para ter mais informações, consulte AWS Formato de descoberta de segurança (ASFF).

Controle

Uma proteção ou contramedida prescrita para um sistema de informações ou uma organização projetada para proteger a confidencialidade, integridade e disponibilidade de suas informações e para atender a um conjunto de requisitos de segurança definidos. Um padrão de segurança está associado a uma coleção de controles.

O termo controle de segurança se refere aos controles que têm um único ID e título de controle em todos os padrões. O termo controle padrão se refere aos controles que têm IDs e títulos de controle específicos do padrão. Atualmente, o Security Hub só é compatível com controles padrão nas regiões da AWS GovCloud (US) Region e da China. Os controles de segurança são compatíveis com em todas as outras regiões.

Ação personalizada

Um mecanismo do Security Hub para enviar descobertas selecionadas para EventBridge o. Uma ação personalizada é criada no Security Hub. Em seguida, é vinculado a uma EventBridge regra. A regra define uma ação específica a ser realizada quando for recebida uma descoberta associada ao ID da ação personalizada. As ações personalizadas podem ser usadas, por exemplo, para enviar uma descoberta específica ou um conjunto pequeno de descobertas a um fluxo de trabalho de resposta ou de correção. Para ter mais informações, consulte the section called “Criar uma ação personalizada (console)”.

Conta de administrador delegado (Organizations)

Em Organizations, a conta de administrador delegado de um serviço é capaz de gerenciar o uso de um serviço para a organização.

No Security Hub, a conta de administrador do Security Hub também é a conta de administrador delegado do Security Hub. Quando a conta de gerenciamento da organização designa pela primeira vez uma conta de administrador do Security Hub, ele designa o Organizations para tornar essa conta a conta de administrador delegado.

A conta de gerenciamento da organização deve então escolher a conta de administrador delegado como a conta de administrador do Security Hub em todas as regiões.

Descoberta

O registro observável de uma verificação de segurança ou detecção relacionada à segurança. O Security Hub gera uma descoberta após concluir uma verificação de segurança de um controle. Elas são chamadas de descobertas de controle. As descobertas também podem vir de integrações de produtos de terceiros.

Para mais informações sobre descobertas no Security Hub, consulte Descobertas.

> **Note**
>
> As descobertas são excluídas 90 dias após a atualização mais recente ou 90 dias após a data de criação, se não ocorrer nenhuma atualização. Para armazenar descobertas por mais de 90 dias, você pode configurar uma regra EventBridge que encaminhe as descobertas para seu bucket do Amazon S3.

Agregação entre regiões

A agregação de descobertas, insights, status de conformidade de controle e pontuações de segurança de regiões vinculadas a uma região de agregação. Em seguida, você pode visualizar todos os seus dados da região de agregação e atualizar as descobertas e insights dessa região.

Consulte Agregação entre regiões.

Descoberta de ingestão

A importação de descobertas para o Security Hub de outros AWS serviços e de fornecedores parceiros terceirizados.

A descoberta de eventos de ingestão inclui novas descobertas e atualizações das descobertas existentes.

Insight

Uma coleção de descobertas relacionadas definidas por uma instrução de agregação e filtros opcionais. Um insight identifica uma área de segurança que requer atenção e intervenção. O Security Hub oferece vários insights gerenciados (padrão) que você não pode modificar.

Você também pode criar insights personalizados do Security Hub para rastrear problemas de segurança exclusivos do seu AWS ambiente e uso. Para ter mais informações, consulte Insights.

Região vinculada

Quando você ativa a agregação entre regiões, uma região vinculada é aquela que agrega descobertas, insights, status de conformidade de controle e pontuações de segurança à região de agregação.

Em uma região vinculada, as páginas Descobertas e Insights contêm descobertas somente dessa região.

Consulte Agregação entre regiões.

Conta-membro

Uma conta que concedeu permissão a uma conta de administrador para visualizar e agir de acordo com suas descobertas.

Uma conta se torna uma conta-membro de uma das seguintes maneiras:

- A conta aceita um convite de outra conta.
- Para uma conta de organização, a conta de administrador do Security Hub habilita a conta como uma conta-membro.

Requisitos relacionados

Um conjunto de requisitos normativos ou do setor que são mapeados para um controle.

Regra

Um conjunto de critérios automatizados que é usado para avaliar se um controle está sendo cumprido. Quando uma regra é avaliada, ela pode ser aprovada ou reprovada. Se a avaliação não puder determinar se a regra será aprovada ou reprovada, a regra estará em um estado de aviso. Se não for possível avaliar a regra, ela estará em um estado indisponível.

Verificação de segurança

Uma point-in-time avaliação específica de uma regra em relação a um único recurso, resultando em um estado aprovado, com falha, aviso ou indisponível. Executar uma verificação de segurança produz uma descoberta.

Conta de administrador do Security Hub

Uma conta da organização que gerencia a associação ao Security Hub de uma organização.

A conta de gerenciamento da organização designa a conta de administrador do Security Hub em cada região. A conta de gerenciamento da organização deve escolher a mesma conta de administrador do Security Hub em todas as regiões.

A conta de administrador do Security Hub também é a conta de administrador delegado do Security Hub no Organizations.

A conta de administrador do Security Hub pode habilitar outras contas da organização como sendo contas-membro. A conta de administrador do Security Hub também pode convidar outras contas para serem contas membros.

Padrão de segurança

Uma instrução publicada em um tópico especificando as características, geralmente mensuráveis e na forma de controles, que devem ser atendidas ou atingidas para estar em conformidade. Os padrões de segurança podem ser baseados em estruturas regulatórias, melhores práticas ou políticas internas da empresa. Um controle pode estar associado a um ou mais padrões compatíveis no Security Hub. Para saber mais sobre padrões de segurança no Security Hub, consulte Padrões e controles.

Gravidade

A severidade atribuída a um controle do Security Hub identifica a importância do controle. A severidade de um controle pode ser Crítica, Alta, Média, Baixa ou Informativa. A severidade atribuída às descobertas de controle é igual à severidade do controle em si. Para saber como o Security Hub atribui severidade a um controle, consulte Atribuir severidade às descobertas de controle.

Status do fluxo de trabalho

O status de uma investigação sobre uma descoberta. Rastrear usando o atributo `Workflow.Status`.

O status do fluxo de trabalho é inicialmente `NEW`. Se você notificou o proprietário do recurso para executar uma ação na descoberta, poderá definir o status do fluxo de trabalho como `NOTIFIED`. Se a descoberta não for um problema e não exigir nenhuma ação, defina o status do fluxo de trabalho como `SUPPRESSED`. Depois de revisar e corrigir uma descoberta, defina o status do fluxo de trabalho como `RESOLVED`.

Por padrão, a maioria das listas de descobertas inclui apenas descobertas com o status de fluxo de trabalho `NEW` ou `NOTIFIED`. As listas de descobertas para controles também incluem descobertas `RESOLVED`.

Para a operação `GetFindings`, é possível incluir um filtro para o status de fluxo de trabalho.

```
"WorkflowStatus": [
    {
        "Comparison": "EQUALS",
        "Value": "RESOLVED"
    }
],
```

O console do Security Hub fornece uma opção para definir o status do fluxo de trabalho para descobertas. Os clientes (ou SIEM, emissão de tíquetes, gerenciamento de incidentes ou ferramentas SOAR que funcionam em nome de um cliente para atualizar as descobertas dos provedores de descobertas) também podem usar `BatchUpdateFindings` para atualizar o status de fluxo de trabalho.

Recomendações antes de ativar o Security Hub

As recomendações a seguir podem ajudar você a começar a usar AWS Security Hub.

Integrando com AWS Organizations

AWS Organizations é um serviço global de gerenciamento de contas que permite AWS aos administradores consolidar e gerenciar centralmente várias Contas da AWS unidades organizacionais (OUs). Ele fornece os atributos de faturamento consolidado e gerenciamento de contas, projetados para atender às necessidades orçamentárias, de segurança e de conformidade. Ele é oferecido sem custo adicional e se integra a vários Serviços da AWS, incluindo Security Hub GuardDuty, Amazon e Amazon Macie.

Para ajudar a automatizar e agilizar o gerenciamento de contas, é altamente recomendável integrar o Security Hub e o AWS Organizations. Você pode se integrar ao Organizations se tiver mais de um Conta da AWS que use o Security Hub.

Para obter instruções sobre como ativar a integração, consulte Integrando o Security Hub com AWS Organizations.

Uso da configuração central

Ao integrar o Security Hub e o Organizations, você tem a opção de usar um recurso chamado configuração central para configurar e gerenciar o Security Hub para sua organização. É altamente recomendável usar a configuração central, pois ela permite que o administrador personalize a cobertura de segurança para a organização. Quando apropriado, o administrador delegado pode permitir que uma conta-membro defina suas próprias configurações de cobertura de segurança.

A configuração central permite que o administrador delegado configure o Security Hub em contas, unidades organizacionais e regiões. O administrador delegado configura o Security Hub criando políticas de configuração. Em uma política de configuração, é possível especificar as configurações a seguir:

- Se o Security Hub está habilitado ou desabilitado
- Quais padrões de segurança são habilitados e desabilitados
- Quais controles de segurança são habilitados e desabilitados
- Se os parâmetros devem ser personalizados para selecionar controles

Como administrador delegado, é possível criar uma única política de configuração para toda a organização ou políticas de configuração diferentes para suas várias contas e unidades organizacionais. Por exemplo, contas de teste e contas de produção podem usar políticas de configuração diferentes.

As contas-membro e unidades organizacionais que usem uma política de configuração são gerenciadas centralmente e só podem ser configuradas pelo administrador delegado. O administrador delegado pode designar contas-membro e unidades organizacionais específicas como autogerenciadas para permitir que o membro defina suas próprias configurações por região.

Para saber mais sobre a configuração central, consulte Como a configuração central funciona.

Configurando AWS Config

AWS Security Hub usa AWS Config regras vinculadas a serviços para realizar verificações de segurança na maioria dos controles.

Para oferecer suporte a esses controles, AWS Config devem estar habilitados em todas as contas, tanto na conta de administrador quanto nas contas de membros, em cada uma em que o Região da AWS Security Hub esteja ativado. Além disso, para cada padrão habilitado, AWS Config deve ser configurado para registrar os recursos necessários para os controles habilitados.

Recomendamos que você ative a gravação de recursos AWS Config antes de habilitar os padrões do Security Hub. Se o Security Hub tentar executar verificações de segurança quando a gravação de recursos estiver desativada, as verificações darão erros.

O Security Hub não AWS Config gerencia para você. Se você já tiver AWS Config habilitado, poderá definir suas configurações por meio do AWS Config console ou das APIs.

Se você habilitar um padrão, mas não tiver ativado AWS Config, o Security Hub tentará criar as AWS Config regras de acordo com o seguinte cronograma:

- No dia em que você habilita o padrão
- No dia seguinte à habilitação do padrão
- 3 dias depois de habilitar o padrão
- 7 dias depois de ativar o padrão (e continuamente a cada 7 dias a partir de então)

Se você usar a configuração central, o Security Hub também tentará criar as AWS Config regras ao reaplicar uma política de configuração que habilite um ou mais padrões.

Habilitando AWS Config

Se você ainda não AWS Config tiver ativado, você pode habilitá-lo de uma das seguintes formas:

- Console ou AWS CLI — Você pode ativar manualmente AWS Config usando o AWS Config console ou AWS CLI. Consulte Conceitos básicos do AWS Config no Guia do desenvolvedor do AWS Config .
- AWS CloudFormation modelo — Se você quiser ativar AWS Config em um grande número de contas, você pode habilitar AWS Config com o CloudFormation modelo Ativar AWS Config. Para acessar esse modelo, consulte modelos de AWS CloudFormation StackSets amostra no Guia AWS CloudFormation do usuário.
- Script do Github — O Security Hub oferece um GitHub script que habilita o Security Hub para várias contas em todas as regiões. Esse script é útil se você não se integrou a Organizações ou se tem contas que não fazem parte da sua organização. Quando você usa esse script para ativar o Security Hub, ele também é ativado automaticamente AWS Config para essas contas.

Para obter mais informações sobre como habilitar AWS Config para ajudá-lo a executar as verificações de segurança do Security Hub, consulte Otimizar AWS ConfigAWS Security Hub para gerenciar com eficiência sua postura de segurança na nuvem.

Ativando a gravação de recursos em AWS Config

Quando você ativa a gravação de recursos AWS Config com as configurações padrão, ela registra todos os tipos de recursos regionais suportados que são AWS Config descobertos no local Região da AWS em que está sendo executado. Você também pode configurar AWS Config para registrar os tipos de recursos globais suportados. Você só precisa registrar recursos globais em uma única região (recomendamos que essa seja sua região inicial se você estiver usando a configuração central).

Se você estiver usando CloudFormation StackSets para habilitar AWS Config, recomendamos que você execute dois diferentes StackSets. Execute um StackSet para registrar todos os recursos, incluindo recursos globais, em uma única região. Execute um segundo StackSet para registrar todos os recursos, exceto os recursos globais em outras regiões.

Você também pode usar a Configuração rápida, um recurso de AWS Systems Manager, para configurar rapidamente o registro de recursos em AWS Config todas as suas contas e regiões. Durante o processo de Configuração Rápida, é possível escolher em qual região gostaria de gravar

recursos globais. Para obter mais informações, consulte o Gravador de configuração do AWS Config no Guia do usuário do AWS Systems Manager .

O controle de segurança Config.1 gerará descobertas com falha em regiões onde os recursos globais não são gravados. Isso é esperado, e é possível usar uma regra de automação para suprimir essas descobertas.

Se você usar o script de várias contas para habilitar o Security Hub, ele habilitará automaticamente a gravação de recursos para todos os recursos, incluindo recursos globais, em todas as regiões. Em seguida, é possível atualizar a configuração para gravar recursos globais em uma única região apenas. Para obter informações, consulte Seleção de quais AWS Config registros de recursos no Guia do AWS Config desenvolvedor.

Para que o Security Hub relate com precisão as descobertas dos controles que dependem de AWS Config regras, você deve habilitar a gravação dos recursos relevantes. Para obter uma lista de controles e seus AWS Config recursos relacionados, consulteAWS Config recursos necessários para gerar resultados de controle.AWS Config permite escolher entre gravação contínua e gravação diária de alterações no estado do recurso. Se você escolher a gravação diária, a AWS Config fornecerá dados de configuração do recurso no final de cada período de 24 horas se houver alterações no estado do recurso. Se não houver alterações, nenhum dado será entregue. Isso pode atrasar a geração das descobertas do Security Hub para controles acionados por alterações até que um período de 24 horas seja concluído.

> **Note**
>
> Para gerar novas descobertas após as verificações de segurança e evitar descobertas obsoletas, você deve ter permissões suficientes para que o perfil do IAM anexado ao gravador de configuração avalie os recursos subjacentes.

Considerações sobre custos

Para obter detalhes sobre os custos associados à gravação de recursos, consulte preços do AWS Security Hub e preços do AWS Config.

O Security Hub pode afetar os custos AWS Config do gravador de configuração ao atualizar o item `AWS::Config::ResourceCompliance` de configuração. As atualizações podem ocorrer sempre que um controle do Security Hub associado a uma AWS Config regra muda de estado de conformidade, é ativado ou desativado ou tem atualizações de parâmetros. Se

você usa o gravador de AWS Config configuração somente para o Security Hub e não usa esse item de configuração para outros fins, recomendamos desativar a gravação no AWS Config console ou AWS CLI. Isso pode reduzir os custos do AWS Config . Você não precisa gravar `AWS::Config::ResourceCompliance` para que as verificações de segurança funcionem no Security Hub.

Habilitar o Security Hub

Há duas formas de habilitar o AWS Security Hub: com a integração com o AWS Organizations ou manualmente.

É altamente recomendável fazer a integração com Organizations para ambientes com várias contas e várias regiões. Se você tiver uma conta independente, será necessário configurar o Security Hub manualmente.

Verificação das permissões necessárias

Depois de se cadastrar na Amazon Web Services (AWS), será necessário habilitar o Security Hub para usar suas capacidades e recursos. Para habilitar o Security Hub, é preciso primeiramente configurar permissões que permitam seu acesso ao console do Security Hub e às operações da API. Você ou seu administrador da AWS podem fazer isso usando o AWS Identity and Access Management (IAM) para anexar a política gerenciada pela AWS chamada `AWSSecurityHubFullAccess` à sua identidade do IAM.

Para habilitar e gerenciar o Security Hub por meio da integração do Organizations, você também deve anexar a política gerenciada pela AWS chamada `AWSSecurityHubOrganizationsAccess`.

Para obter mais informações, consulte AWS políticas gerenciadas para o AWS Security Hub.

Habilitação do Security Hub com a integração do Organizations

Para começar a usar o Security Hub com o AWS Organizations, a conta de gerenciamento do AWS Organizations para a organização designa uma conta como conta de administrador delegado do Security Hub para a organização. O Security Hub é habilitado automaticamente na conta de administrador delegado na região atual.

Escolha seu método preferido e siga as etapas para designar o administrador delegado.

Security Hub console

Para designar o administrador delegado do Security Hub durante a integração

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.
2. Escolha Ir para o Security Hub. Você será solicitado a fazer login na conta de gerenciamento do Organizations.

3. Na página Designar administrador delegado, na seção Conta de administrador delegado, especifique a conta de administrador delegado. Recomendamos escolher o mesmo administrador delegado que você definiu para outros serviços de segurança e conformidade da AWS.
4. Escolha Definir administrador delegado.

Security Hub API

Invoque a API `EnableOrganizationAdminAccount` da conta de gerenciamento do Organizations. Forneça o ID da Conta da AWS da conta de administrador delegado do Security Hub.

AWS CLI

Execute o comando `enable-organization-admin-account` a partir da conta de gerenciamento do Organizations. Forneça o ID da Conta da AWS da conta de administrador delegado do Security Hub.

Exemplo de comando:

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

Para obter mais informações sobre a integração com o Organizations, consulte Integrando o Security Hub com AWS Organizations.

Depois de designar o administrador delegado, recomendamos que você continue configurando o Security Hub com a configuração central. O console solicita que você faça isso. Ao usar a configuração central, é possível simplificar o processo de habilitação e configuração do Security Hub para sua organização e garantir que sua organização tenha a cobertura de segurança adequada.

A configuração central permite que o administrador delegado personalize o Security Hub em várias contas e regiões da organização, em vez de configurar região por região. É possível criar uma política de configuração para toda a organização ou criar políticas de configuração diferentes para contas e OUs diferentes. As políticas especificam se o Security Hub está habilitado ou desabilitado nas contas associadas e quais padrões e controles de segurança estão habilitados.

O administrador delegado pode designar contas como sendo gerenciadas centralmente ou autogerenciadas. As contas gerenciadas centralmente só podem ser configuradas pelo administrador delegado. As contas autogerenciadas podem especificar suas próprias configurações.

Se você não usar a configuração central, o administrador delegado terá uma capacidade mais limitada de configurar o Security Hub. Para obter mais informações, consulte Gerenciando contas com AWS Organizations.

Habilitar o Security Hub

Você deve habilitar o Security Hub manualmente se tiver uma conta independente ou se não fizer integração com o AWS Organizations. Contas autônomas não podem ser integradas ao AWS Organizations, e devem usar a habilitação manual.

Ao habilitar o Security Hub manualmente, você designa uma conta de administrador do Security Hub e convida outras contas para se tornarem contas-membro. A relação administrador-membro é estabelecida quando uma conta-membro em potencial aceita o convite da conta.

Escolha seu método preferido e siga as etapas para habilitar o Security Hub. Ao habilitar o Security Hub no console, você também tem a opção de habilitar os padrões de segurança suportados.

Security Hub console

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.
2. Ao abrir o console do Security Hub pela primeira vez, escolha Ir para o Security Hub.
3. Na página de boas-vindas, a seção padrões de segurança lista os padrões de segurança com suporte no Security Hub.

   Marque a caixa de seleção de um padrão para habilitá-lo e desmarque a caixa de seleção para desabilitá-lo.

   É possível habilitar ou desabilitar um padrão ou seus controles individuais a qualquer momento. Para obter informações sobre o gerenciamento de padrões e controles de segurança, consulte Controles e padrões de segurança no AWS Security Hub.
4. Selecione Enable Security Hub (Habilitar o Security Hub).

Security Hub API

Invoque a API `EnableSecurityHub`. Ao habilitar o Security Hub pela API, ele habilitará automaticamente os padrões de segurança padrão a seguir:

- AWS Práticas Recomendadas de Segurança Básica

- Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0

Se você não quiser habilitar esses padrões, defina `EnableDefaultStandards` como `false`.

Você também pode usar o parâmetro `Tags` para atribuir valores de tag ao recurso do hub.

AWS CLI

Execute o comando `enable-security-hub`. Para ativar os padrões, inclua `--enable-default-standards`. Para não ativar os padrões, inclua `--no-enable-default-standards`. Os padrões de segurança padrão são os seguintes:

- AWS Práticas Recomendadas de Segurança Básica
- Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0

```
aws securityhub enable-security-hub [--tags <tag values>] [--enable-default-
standards | --no-enable-default-standards]
```

Exemplo

```
aws securityhub enable-security-hub --enable-default-standards --tags
 '{"Department": "Security"}'
```

Script de habilitação de várias contas

> **Note**
>
> Em vez desse script, recomendamos usar a configuração central para habilitar e configurar o Security Hub em várias contas e regiões.

O script de habilitação de várias contas do Security Hub no GitHub permite que você habilite o Security Hub em todas as contas e regiões. O script também automatiza o processo de envio de convites para contas de membros e habilitação de AWS Config.

O script ativa automaticamente a gravação de recursos para todos os recursos, incluindo recursos globais, em todas as regiões. Ele não limita o registro de recursos globais a uma única região.

Há um script correspondente para desativar o Security Hub em todas as contas e regiões.

Próximas etapas após a habilitação do Security Hub

Depois de habilitar o Security Hub, recomendamos habilitar os padrões e controles de segurança, que são importantes para suas necessidades de segurança. Depois de habilitar os controles, o Security Hub começa a executar verificações de segurança e a gerar descobertas de controle. Você também pode aproveitar as integrações entre o Security Hub e outros Serviços da AWS e soluções de terceiros para ver suas descobertas no Security Hub.

Como a configuração central funciona

A configuração central é um recurso do Security Hub que ajuda você a configurar e a gerenciar o Security Hub em várias Contas da AWS e Regiões da AWS. Para usar a configuração central, você deve primeiro integrar o Security Hub AWS Organizations e. É possível integrar os serviços criando uma organização e designando uma conta delegada de administrador do Security Hub para a organização.

Na conta delegada do administrador do Security Hub, é possível especificar como o serviço, os padrões de segurança e os controles de segurança do Security Hub são configurados nas contas da sua organização e unidades organizacionais (OUs) em todas as regiões. É possível definir essas configurações em apenas algumas etapas a partir de uma região primária, chamada de região inicial. Se você não usa a configuração central, deve configurar o Security Hub separadamente em cada conta e região.

Quando você usa a configuração central, o administrador delegado pode escolher quais contas e OUs configurar. Se o administrador delegado designar uma conta-membro ou OU como autogerenciada, o membro poderá definir suas próprias configurações separadamente em cada região. Se o administrador delegado designar uma conta-membro ou OU como gerenciada centralmente, somente o administrador delegado poderá configurar a conta-membro ou OU em todas as regiões. É possível designar todas as contas e OUs em sua organização como gerenciadas centralmente, todas autogerenciadas, ou uma combinação de ambas.

Para configurar contas gerenciadas centralmente, o administrador delegado usa políticas de configuração do Security Hub. As políticas de configuração permitem que o administrador delegado especifique se o Security Hub está habilitado ou desabilitado e quais padrões e controles estão habilitados e desabilitados. Elas também podem ser utilizados para personalizar parâmetros de determinados controles.

As políticas de configuração entram em vigor na região inicial e em todas as regiões vinculadas. O administrador delegado especifica a região inicial da organização e as regiões vinculadas antes de começar a usar a configuração central. O administrador delegado pode criar uma única política de configuração para toda a organização ou criar diversas políticas de configuração para definir configurações variáveis para diferentes contas e UOs.

Esta seção fornece uma visão geral da configuração central.

Benefícios da configuração central

Os benefícios da configuração central incluem os seguintes:

Simplificar a configuração do serviço e dos recursos do Security Hub

Quando você usa a configuração central, o Security Hub orienta você no processo de configuração das práticas recomendadas de segurança para sua organização. Ele também implanta automaticamente as políticas de configuração resultantes em contas e OUs especificadas. Se você tiver configurações existentes do Security Hub, como habilitar automaticamente novos controles de segurança, poderá usá-las como ponto de partida para suas políticas de configuração. Além disso, a página Configuração no console do Security Hub exibe um resumo em tempo real de suas políticas de configuração e quais contas e OUs usam cada política.

Configurar entre contas e regiões

É possível usar a configuração central para configurar o Security Hub em várias contas e regiões. Isso ajuda a garantir que cada parte da sua organização mantenha uma configuração consistente e uma cobertura de segurança adequada.

Acomodar configurações diferentes em contas e OUs diferentes

Com a configuração central, é possível optar por configurar as contas e OUs da sua organização de maneiras diferentes. Por exemplo, suas contas de teste e contas de produção podem exigir configurações diferentes. Você também pode criar uma política de configuração que abranja novas contas quando elas ingressarem na organização.

Evitar desvios na configuração

O desvio de configuração ocorre quando um usuário faz uma alteração em um serviço ou recurso que entra em conflito com as seleções do administrador delegado. A configuração central evita esse desvio. Quando você designa uma conta ou OU como gerenciada centralmente, ela poderá ser configurada somente pelo administrador delegado da organização. Se você preferir que uma conta ou OU específica defina suas próprias configurações, é possível designá-la como autogerenciada.

Quem deveria usar a configuração central?

A configuração central é mais benéfica para AWS ambientes que incluem várias contas do Security Hub. Ela foi projetada para ajudar você a gerenciar de forma central o Security Hub para várias contas.

É possível usar a configuração central para configurar o serviço, os padrões de segurança e os controles de segurança do Security Hub. Também é possível usá-la para personalizar os parâmetros de determinados controles. Para obter mais informações sobre padrões e controles, consulte Controles e padrões de AWS segurança no Security Hub.

Termos e conceitos da configuração central

Compreender os termos e conceitos-chave a seguir pode ajudá-lo a usar a configuração central do Security Hub.

Configuração central

Um recurso do Security Hub que ajuda a conta delegada do administrador do Security Hub de uma organização a configurar o serviço, os padrões de segurança e os controles de segurança do Security Hub em várias contas e regiões. Para definir essas configurações, o administrador delegado cria e gerencia as políticas de configuração do Security Hub para contas gerenciadas centralmente em sua organização. As contas autogerenciadas podem definir suas próprias configurações separadamente em cada região. Para usar a configuração central, você deve integrar o Security Hub AWS Organizations e.

Região inicial

A Região da AWS partir da qual o administrador delegado configura centralmente o Security Hub, criando e gerenciando políticas de configuração. As políticas de configuração entram em vigor na região inicial e em todas as regiões vinculadas.

A região inicial também serve como a região de agregação do Security Hub, recebendo descobertas, insights e outros dados das regiões vinculadas.

As regiões que AWS foram introduzidas em ou após 20 de março de 2019 são conhecidas como regiões opcionais. Uma região de adesão não pode ser a região inicial, mas pode ser uma região vinculada. Para obter uma lista de regiões de adesão, consulte Considerações antes de habilitar e desabilitar regiões no Guia de referência de gerenciamento de contas da AWS .

Região vinculada

E Região da AWS isso é configurável a partir da região de origem. As políticas de configuração são criadas pelo administrador delegado na região inicial. As políticas entram em vigor na região inicial e em todas as regiões vinculadas. Você deve especificar pelo menos uma região vinculada para usar a configuração central.

Uma região vinculada também envia descobertas, insights e outros dados para a região inicial.

As regiões que AWS foram introduzidas em ou após 20 de março de 2019 são conhecidas como regiões opcionais. Você deve habilitar essa região para uma conta antes que uma política de configuração possa ser aplicada a ela. A conta de gerenciamento do Organizations pode habilitar regiões de adesão para uma conta-membro. Para obter mais informações, consulte Especificar qual Regiões da AWS conta pode ser usada no Guia de referência de gerenciamento de AWS contas.

Política de configuração do Security Hub

Um conjunto de configurações do Security Hub que o administrador delegado pode definir para contas gerenciadas centralmente. Isso inclui:

- Se o Security Hub deve ser habilitado ou desabilitado.
- Se um ou mais padrões de segurança devem ser habilitados.
- Quais controles de segurança a habilitar dentre todos os padrões habilitados. O administrador delegado pode fazer isso fornecendo uma lista de controles específicos que devem ser habilitados, e o Security Hub desabilitará todos os outros controles (incluindo novos controles quando eles são lançados). De forma alternativa, o administrador delegado pode fornecer uma lista de controles específicos que devem ser desabilitados, e o Security Hub habilitará todos os outros controles (incluindo novos controles quando eles são lançados).
- Opcionalmente, personalize os parâmetros para selecionar controles habilitados dentre os padrões habilitados.

Uma política de configuração entra em vigor na região inicial e em todas as regiões vinculadas depois de ser associada a pelo menos uma conta, unidade organizacional (OU) ou raiz.

No console do Security Hub, o administrador delegado pode escolher a política de configuração recomendada do Security Hub ou criar políticas de configuração personalizadas. Com a API do Security Hub e AWS CLI, o administrador delegado só pode criar políticas de configuração personalizadas. O administrador delegado pode criar no máximo 20 políticas de configuração personalizadas.

Na política de configuração recomendada, o Security Hub, o padrão Práticas Recomendadas de Segurança Básica (FSBP) da AWS e todos os controles de FSBP novos e existentes estão habilitados. Os controles que aceitam parâmetros usam os valores padrão. A política de configuração recomendada se aplica a toda a organização.

Para aplicar configurações diferentes à organização ou aplicar políticas de configuração diferentes a contas e OUs diferentes, crie uma política de configuração personalizada.

Configuração local

O tipo de configuração padrão para uma organização, depois de integrar o Security Hub e. AWS Organizations Com a configuração local, o administrador delegado pode optar por habilitar automaticamente o Security Hub e os padrões de segurança padrão em novas contas da organização na região atual. Se o administrador delegado habilitar automaticamente os padrões padrão, todos os controles que fazem parte desses padrões também serão habilitados automaticamente com parâmetros padrão para as novas contas da organização. Essas configurações não se aplicam às contas existentes, portanto, é possível alterar a configuração depois que uma conta ingressa na organização. A desabilitação de controles específicos que fazem parte dos padrões padrão e a configuração de padrões e controles adicionais devem ser feitas separadamente em cada conta e região.

A configuração local não oferece suporte ao uso de políticas de configuração. Para usar políticas de configuração, você deve alternar para a configuração central.

Gerenciamento manual de contas

Se você não integrar o Security Hub AWS Organizations ou tiver uma conta independente, deverá especificar as configurações para cada conta separadamente em cada região. O gerenciamento manual de contas não oferece suporte ao uso de políticas de configuração.

APIs da configuração central

Operações do Security Hub que somente o administrador delegado do Security Hub pode usar na região inicial para gerenciar políticas de configuração para contas gerenciadas centralmente. As operações incluem:

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`
- `UpdateConfigurationPolicy`

- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

APIs específicas da conta

Operações do Security Hub que podem ser usadas para habilitar ou desabilitar o Security Hub, padrões e controles em uma account-by-account base. Essas operações são usadas em cada região individual.

As contas autogerenciadas podem usar operações específicas da conta para definir suas próprias configurações. As contas gerenciadas centralmente não podem usar as operações a seguir, específicas da conta na região inicial e nas regiões vinculadas. Nessas regiões, apenas o administrador delegado pode configurar contas gerenciadas centralmente por meio de operações de configuração central e políticas de configuração.

- `BatchDisableStandards`
- `BatchEnableStandards`
- `BatchUpdateStandardsControlAssociations`
- `DisableSecurityHub`
- `EnableSecurityHub`
- `UpdateStandardsControl`

Para verificar o status da conta, o proprietário de uma conta gerenciada centralmente pode usar `Get` qualquer `Describe` operação da API do Security Hub.

Se você usar a configuração local ou o gerenciamento manual de contas, em vez da configuração central, essas operações específicas da conta poderão ser usadas.

Contas autogerenciadas também podem ser usadas `*Invitations` e `*Members` operadas. No entanto, recomendamos que as contas autogerenciadas não usem essas operações. As associações de políticas podem falhar se a conta de um membro tiver seus próprios membros que fazem parte de uma organização diferente da do administrador delegado.

Unidade organizacional (UO)

No AWS Organizations Security Hub, um contêiner para um grupo de Contas da AWS. Uma unidade organizacional (OU) também pode conter outras OUs, permitindo que você crie uma

hierarquia parecida com uma árvore de cabeça para baixo, com uma OU principal na parte superior e ramificações de OUs que se propagam para níveis inferiores, terminando em contas que são as folhas da árvore. Uma UO pode ter exatamente um pai, e, atualmente, cada conta pode ser um membro de exatamente uma UO.

Você pode gerenciar OUs em AWS Organizations ou AWS Control Tower. Para obter mais informações, consulte Gerenciamento de unidades organizacionais no Guia do usuário do AWS Organizations ou Governo de organizações e contas com o AWS Control Tower no Guia do usuário do AWS Control Tower .

O administrador delegado pode associar políticas de configuração a contas ou OUs específicas ou à raiz para cobrir todas as contas e OUs em uma organização.

Gerenciada centralmente

Uma conta, OU ou raiz que somente o administrador delegado pode configurar em todas as regiões usando políticas de configuração.

A conta de administrador delegado especifica se uma conta é gerenciada centralmente. O administrador delegado também pode alterar o status de uma conta de gerenciada centralmente para autogerenciada, ou vice-versa.

Autogerenciado

Uma conta, OU ou raiz que gerencia suas próprias configurações do Security Hub. Uma conta autogerenciada usa operações específicas da conta para configurar o Security Hub separadamente em cada região. Isso contrasta com as contas gerenciadas centralmente, que só podem ser configuradas pelo administrador delegado em todas as regiões por meio de políticas de configuração.

A conta de administrador delegado especifica se uma conta é autogerenciada. A conta de administrador delegado também pode alterar o status de uma conta de autogerenciada para gerenciada centralmente, ou vice-versa.

O administrador delegado pode aplicar um comportamento autogerenciado a uma conta ou UO. Como alternativa, uma conta ou OU pode herdar o comportamento autogerenciado de um dos pais. A própria conta de administrador delegado pode ser uma conta autogerenciada.

Associação de políticas de configuração

Um link entre uma política de configuração e uma conta, unidade organizacional (OU) ou uma raiz. Quando existe uma associação de política, a conta, a OU ou a raiz usam as configurações definidas pela política de configuração. Existe uma associação em qualquer um destes casos:

- Quando o administrador delegado aplica diretamente uma política de configuração a uma conta, UO ou raiz
- Quando uma conta ou OU herda uma política de configuração de uma OU principal ou da raiz

Uma associação existe até que uma configuração diferente seja aplicada ou herdada.

Política de configuração aplicada

Um tipo de associação de política de configuração na qual o administrador delegado aplica diretamente uma política de configuração às contas de destino, OUs ou à raiz. Os destinos são configurados da forma que a política de configuração define, e somente o administrador delegado pode alterar sua configuração. Se aplicada à raiz, a política de configuração afeta todas as contas e OUs na organização que não usem uma configuração diferente por meio de aplicação ou herança do pai mais próximo.

O administrador delegado também pode aplicar uma configuração autogerenciada a contas específicas, OUs ou à raiz.

Política de configuração herdada

Um tipo de associação de política de configuração em que uma conta ou OU adota a configuração da OU principal mais próxima ou da raiz. Se uma política de configuração não for aplicada diretamente a uma conta ou UO, ela herdará a configuração do pai mais próximo. Todos os elementos de uma política são herdados. Em outras palavras, uma conta ou OU não pode escolher herdar seletivamente somente partes de uma política. Se o pai mais próximo for autogerenciado, a conta ou OU filha herdará o comportamento autogerenciado do pai.

A herança não pode substituir uma configuração aplicada. Ou seja, se uma política de configuração ou configuração autogerenciada for aplicada diretamente a uma conta ou OU, ela usará essa configuração e não herdará a configuração do pai.

Raiz

No Security Hub AWS Organizations e no Security Hub, o nó principal de uma organização. Se o administrador delegado aplicar uma política de configuração à raiz, a política será associada a todas as contas e OUs da organização, a menos que elas usem uma política diferente, por meio de aplicação ou herança, ou sejam designadas como autogerenciadas. Se o administrador designar a raiz como autogerenciada, todas as contas e OUs na organização serão autogerenciadas, a menos que usem uma política de configuração por meio de aplicação ou herança. Se a raiz for autogerenciada e nenhuma política de configuração existir atualmente, todas as novas contas na organização manterão suas configurações atuais.

As novas contas que ingressem em uma organização ficarão sob a raiz até serem atribuídas a uma OU específica. Se uma nova conta não for atribuída a uma OU, ela herdará a configuração raiz, a menos que o administrador delegado a designe como uma conta autogerenciada.

Comece a usar a configuração central

A conta de administrador delegado do AWS Security Hub pode usar a configuração central para configurar o Security Hub, padrões e controles para várias contas e unidades organizacionais (OUs) nas Regiões da AWS.

Esta seção explica os pré-requisitos da configuração central e como começar a usá-la.

Pré-requisitos para a configuração central

Antes de começar a usar a configuração central, você deverá integrar o Security Hub ao AWS Organizations e designar uma região inicial. Se você usa o console do Security Hub, esses pré-requisitos são incluídos no fluxo de trabalho de adesão para configuração central.

Integrar ao Organizations

Você precisa integrar o Security Hub e o Organizations para usar a configuração central.

Para integrar esses serviços, você começa criando uma organização no Organizations. A partir da conta de gerenciamento do Organizations, você designa uma conta de administrador delegado do Security Hub. Para obter instruções, consulte Integrando o Security Hub com AWS Organizations.

Certifique-se de designar seu administrador delegado na sua região inicial pretendida. Quando você começa a usar a configuração central, o mesmo administrador delegado também é definido automaticamente em todas as regiões vinculadas. A conta de gerenciamento do Organizations não pode ser definida como uma conta de administrador delegado.

Important

Ao usar a configuração central, você não pode usar o console do Security Hub ou as APIs do Security Hub para alterar ou remover a conta do administrador delegado. Se a conta de gerenciamento do Organizations usar as APIs do AWS Organizations para alterar ou remover o administrador delegado do Security Hub, o Security Hub interromperá automaticamente a configuração central. Suas políticas de configuração também serão desassociadas e

excluídas. As contas-membro retêm as configurações que tinham antes de o administrador delegado ser alterado ou removido.

Designar uma região inicial

Você deve designar uma região inicial para usar a configuração central. A região inicial é aquela a partir da qual o administrador delegado configura a organização.

Para usar a configuração central, você deve especificar pelo menos uma região vinculada que seja configurável a partir da região inicial.

> **Note**
>
> A região inicial não pode ser uma região que a AWS tenha designado como uma região de adesão. Uma região de adesão é desabilitada por padrão. Para obter uma lista de regiões de adesão, consulte Considerações antes de habilitar e desabilitar regiões no Guia de referência de gerenciamento de contas da AWS.

O administrador delegado pode criar e gerenciar políticas de configuração somente a partir da região inicial. As políticas de configuração entram em vigor na região inicial e em todas as regiões vinculadas. Você não pode criar uma política de configuração que seja aplicada somente a um subconjunto dessas regiões, e não a outras.

A região inicial também é a sua região de agregação do Security Hub, que recebe descobertas, insights e outros dados das regiões vinculadas.

Se você já definiu uma região de agregação para a agregação entre regiões, essa é sua região inicial padrão para a configuração central. É possível alterar a região inicial antes de começar a usar a configuração central excluindo seu agregador de descobertas atual e criando um novo na região inicial desejada. Um agregador de descobertas é um recurso do Security Hub que especifica a região inicial e as regiões vinculadas.

Para designar uma região inicial, siga as etapas para definir uma região de agregação. Se você já tem uma região inicial, pode invocar a API GetFindingAggregator para ver detalhes sobre ela, incluindo quais regiões estão atualmente vinculadas a ela.

Iniciar a configuração central

Escolha seu método preferido e siga as etapas para começar a usar a configuração central para sua organização.

Security Hub console

Para configurar centralmente sua organização

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Configurações e Configuração. Em seguida, escolha Iniciar configuração central.

   Se você estiver se integrando ao Security Hub, escolha Ir para o Security Hub.
3. Na página Designar administrador delegado, selecione sua conta de administrador delegado ou insira o ID da conta. Se aplicável, recomendamos escolher o mesmo administrador delegado que você definiu para outros serviços de segurança e conformidade da AWS. Escolha Definir administrador delegado.
4. Na página Centralizar organização, na seção Regiões, selecione sua região inicial. Você precisa fazer login na região inicial para prosseguir. Se você já definiu uma região de agregação para a agregação entre regiões, ela será exibida como a região inicial. Para alterar a região inicial, escolha Editar configurações da região. Em seguida, será possível selecionar sua região inicial preferida e retornar a esse fluxo de trabalho.
5. Selecione ao menos uma região para vincular à região inicial. Opcionalmente, escolha se você deseja vincular automaticamente as futuras regiões com suporte à região inicial. As regiões que você selecionar aqui poderão ser configuradas a partir da região inicial pelo administrador delegado. As políticas de configuração entram em vigor na sua região inicial e em todas as regiões vinculadas.
6. Escolha Confirmar e continuar.
7. Agora é possível usar a configuração central. Continue seguindo as instruções do console para criar sua primeira política de configuração. Se você ainda não estiver pronto para criar uma política de configuração, escolha Ainda não estou pronto para configurar. É possível criar uma política posteriormente escolhendo Configurações e Configuração no painel de navegação. Para obter instruções sobre como criar uma política de configuração, consulte Criação e associação de políticas de configuração do Security Hub.

Security Hub API

Para configurar centralmente o Security Hub

1. Usando as credenciais da conta do administrador delegado, invoque a API UpdateOrganizationConfiguration a partir da região inicial.
2. Veja o campo `AutoEnable` no `false`.
3. Defina o campo `ConfigurationType` no objeto `OrganizationConfiguration` como `CENTRAL`. Essa ação:
   - Designa a conta de chamada como o administrador delegado do Security Hub em todas as regiões vinculadas.
   - Habilita o Security Hub na conta do administrador delegado em todas as regiões vinculadas.
   - Designa a conta de chamada como o administrador delegado do Security Hub para contas novas e existentes que usem o Security Hub e pertençam à organização. Isso ocorre na região inicial e em todas as regiões vinculadas. A conta de chamada será definida como o administrador delegado para novas contas da organização somente se elas estiverem associadas a uma política de configuração que tenha o Security Hub habilitado. A conta de chamada será definida como o administrador delegado das contas existentes da organização somente se elas já tiverem o Security Hub habilitado.
   - Define AutoEnable como `false` em todas as regiões vinculadas e define AutoEnableStandards como `NONE` na região inicial e em todas as regiões vinculadas. Esses parâmetros não são relevantes nas regiões inicial e vinculadas quando você usa a configuração central, mas é possível habilitar automaticamente o Security Hub e os padrões de segurança padrão nas contas da organização por meio do uso de políticas de configuração.
4. Agora é possível usar a configuração central. O administrador delegado pode criar políticas de configuração para configurar o Security Hub na sua organização. Para obter instruções sobre como criar uma política de configuração, consulte Criação e associação de políticas de configuração do Security Hub.

Exemplo de solicitação de API:

```
{
    "AutoEnable": false,
```

```
    "OrganizationConfiguration": {
        "ConfigurationType": "CENTRAL"
    }
}
```

AWS CLI

Para configurar centralmente o Security Hub

1. Usando as credenciais da conta do administrador delegado, execute o comando update-organization-configuration a partir da região inicial.
2. Inclua o parâmetro `no-auto-enable`.
3. Defina o campo `ConfigurationType` no objeto `organization-configuration` como `CENTRAL`. Essa ação:
   - Designa a conta de chamada como o administrador delegado do Security Hub em todas as regiões vinculadas.
   - Habilita o Security Hub na conta do administrador delegado em todas as regiões vinculadas.
   - Designa a conta de chamada como o administrador delegado do Security Hub para contas novas e existentes que usem o Security Hub e pertençam à organização. Isso ocorre na região inicial e em todas as regiões vinculadas. A conta de chamada será definida como o administrador delegado para novas contas da organização somente se elas estiverem associadas a uma política de configuração que tenha o Security Hub habilitado. A conta de chamada será definida como o administrador delegado das contas existentes da organização somente se elas já tiverem o Security Hub habilitado.
   - Define a opção de habilitação automática como no-auto-enable em todas as regiões vinculadas e define auto-enable-standards como `NONE` na região inicial e em todas as regiões vinculadas. Esses parâmetros não são relevantes nas regiões inicial e vinculadas quando você usa a configuração central, mas é possível habilitar automaticamente o Security Hub e os padrões de segurança padrão nas contas da organização por meio do uso de políticas de configuração.
4. Agora é possível usar a configuração central. O administrador delegado pode criar políticas de configuração para configurar o Security Hub na sua organização. Para obter instruções sobre como criar uma política de configuração, consulte Criação e associação de políticas de configuração do Security Hub.

Exemplo de comando:

```
aws securityhub --region us-east-1 update-organization-configuration \
--no-auto-enable \
--organization-configuration '{"ConfigurationType": "CENTRAL"}'
```

Escolha do tipo de gerenciamento de contas e OUs

Quando você usa a configuração central, o administrador AWS Security Hub delegado pode designar cada conta da organização e unidade organizacional (OU) como gerenciada centralmente ou autogerenciada. O tipo de gerenciamento de uma conta ou OU determina como é possível especificar e alterar suas configurações do Security Hub.

Uma conta autogerenciada ou OU pode definir suas próprias configurações do Security Hub separadamente em cada uma Região da AWS. O administrador delegado não pode definir as configurações do Security Hub para uma conta ou OU autogerenciada, e as políticas de configuração não podem ser associadas a elas. Por outro lado, somente o administrador delegado pode definir as configurações do Security Hub para contas e OUs gerenciadas centralmente na região inicial e em regiões vinculadas. As políticas de configuração podem ser associadas a contas e OUs gerenciadas centralmente.

O administrador delegado pode alternar o status de uma conta ou OU entre autogerenciada e gerenciada centralmente. Por padrão, todas as contas e OUs são autogerenciadas quando você inicia a configuração central por meio da API do Security Hub. No console, o tipo de gerenciamento dependerá da sua primeira política de configuração. As contas e OUs que você associa à sua primeira política são gerenciadas centralmente. Outras contas e OUs são autogerenciadas por padrão.

Se você associar uma política de configuração a uma conta autogerenciada, a política substituirá a designação autogerenciada. A conta é gerenciada centralmente e adota as configurações refletidas na política de configuração.

Contas filhas e OUs podem herdar o comportamento autogerenciado de uma conta pai autogerenciada, da mesma forma que contas filhas e OUs podem herdar políticas de configuração de uma conta pai gerenciada centralmente. Para ter mais informações, consulte Associação de políticas por meio de aplicação e herança.

Uma conta autogerenciada ou OU não pode herdar uma política de configuração de um nó pai ou da raiz. Por exemplo, se você quiser que todas as contas e OUs da sua organização herdem uma política de configuração da raiz, você deve alterar o tipo de gerenciamento dos nós autogerenciados para gerenciados centralmente.

Especificando configurações para contas autogerenciadas

As contas autogerenciadas devem definir suas próprias configurações separadamente em cada região.

Os proprietários de contas autogerenciadas podem invocar as seguintes operações da API do Security Hub em cada região para definir suas configurações:

- `EnableSecurityHub` e `DisableSecurityHub` para habilitar ou desabilitar o serviço Security Hub
- `BatchEnableStandards` e `BatchDisableStandards` para habilitar ou desabilitar padrões
- `BatchUpdateStandardsControlAssociations` ou `UpdateStandardsControl` para habilitar ou desabilitar

Contas autogerenciadas também podem ser usadas `*Invitations` e `*Members` operadas. No entanto, recomendamos que as contas autogerenciadas não usem essas operações. As associações de políticas podem falhar se a conta de um membro tiver seus próprios membros que fazem parte de uma organização diferente da do administrador delegado.

Para obter descrições das ações da API do Security Hub, consulte a Referência da API do AWS Security Hub .

As contas autogerenciadas também podem usar o console do Security Hub ou AWS CLI definir suas configurações em cada região.

As contas autogerenciadas não podem invocar nenhuma API relacionada às políticas de configuração e associações de políticas do Security Hub. Somente o administrador delegado pode invocar APIs de configuração central e usar políticas de configuração para configurar contas gerenciadas centralmente.

Escolha do tipo de gerenciamento de contas e OUs

Escolha seu método preferido e siga as etapas para designar uma conta ou OU como gerenciada centralmente ou autogerenciada.

Security Hub console

Para escolher o tipo de gerenciamento de uma conta ou OU

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

   Faça login usando as credenciais da conta do administrador delegado do Security Hub na região inicial.
2. Escolher configuração.
3. Na guia Organização, selecione a conta ou OU de destino. Selecione a opção Editar.
4. Na página Definir configuração, em Tipo de gerenciamento, escolha Gerenciada centralmente se quiser que o administrador delegado configure a conta ou OU de destino. Em seguida, escolha Aplicar uma política específica se quiser associar uma política de configuração existente ao destino. Escolha Herdar da minha organização se desejar que o destino herde a configuração do pai mais próximo. Escolha Autogerenciado se desejar que a conta ou OU defina suas próprias configurações.
5. Escolha Próximo. Revise suas alterações e escolha Salvar.

Security Hub API

Para escolher o tipo de gerenciamento de uma conta ou OU

1. Invoque a API StartConfigurationPolicyAssociation a partir da conta de administrador delegado do Security Hub na região inicial.
2. No campo `ConfigurationPolicyIdentifier`, forneça `SELF_MANAGED_SECURITY_HUB` se você deseja que a conta ou OU controle suas próprias configurações. Forneça o nome do recurso da Amazon (ARN) ou o ID da política de configuração relevante se quiser que o administrador delegado controle as configurações da conta ou da OU.
3. Para o `Target` campo, forneça o Conta da AWS ID, ID da OU ou ID raiz do destino cujo tipo de gerenciamento você deseja alterar. Isso associará o comportamento autogerenciado ou a política de configuração especificada ao destino. As contas filhas do destino podem herdar o comportamento autogerenciado ou a política de configuração.

Exemplo de solicitação de API para designar uma conta autogerenciada:

```
{
    "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
```

```
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

Para escolher o tipo de gerenciamento de uma conta ou OU

1. Execute o comando start-configuration-policy-association a partir da conta de administrador delegado do Security Hub na região inicial.
2. No campo `configuration-policy-identifier`, forneça `SELF_MANAGED_SECURITY_HUB` se você deseja que a conta ou OU controle suas próprias configurações. Forneça o nome do recurso da Amazon (ARN) ou o ID da política de configuração relevante se quiser que o administrador delegado controle as configurações da conta ou da OU.
3. Para o `target` campo, forneça o Conta da AWS ID, ID da OU ou ID raiz do destino cujo tipo de gerenciamento você deseja alterar. Isso associará o comportamento autogerenciado ou a política de configuração especificada ao destino. As contas filhas do destino podem herdar o comportamento autogerenciado ou a política de configuração.

Exemplo de comando para designar uma conta autogerenciada:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
--target '{"AccountId": "123456789012"}'
```

Como as políticas de configuração do Security Hub funcionam

A conta de administrador delegado pode criar políticas de AWS Security Hub configuração para configurar o Security Hub, padrões de segurança e controles de segurança em sua organização. Depois de criar uma política de configuração, o administrador delegado pode associá-la a contas, unidades organizacionais (OUs) ou à raiz. O administrador delegado também pode visualizar, editar ou excluir políticas de configuração.

Considerações sobre políticas

Antes de criar uma política de configuração no Security Hub, considere os detalhes a seguir.

- As políticas de configuração devem ser associadas para entrarem em vigor: depois de criar uma política de configuração, é possível associá-la a uma ou mais contas, unidades organizacionais (OUs) ou à raiz. Contas e OUs podem estar associadas a uma política de configuração por meio de aplicação direta ou herança de um pai.
- Uma conta ou OU só pode ser associada a uma política de configuração — Para evitar configurações conflitantes, uma conta ou OU só pode ser associada a uma política de configuração por vez. Como alternativa, uma conta ou OU pode ser autogerenciada.
- As políticas de configuração são completas: as políticas de configuração fornecem uma especificação completa das configurações. Por exemplo, uma conta filha não pode aceitar configurações para alguns controles de uma política e configurações para outros controles de outra política. Ao associar uma política a uma conta filha, verifique se a política especifica todas as configurações que você deseja que a conta filha use.
- As políticas de configuração não podem ser revertidas — Não há opção de reverter uma política de configuração depois de associá-la a contas ou OUs. Por exemplo, se você associar uma política de configuração que desabilita CloudWatch controles a uma conta específica e, em seguida, dissociar essa política, os CloudWatch controles continuarão desativados nessa conta. Para ativar CloudWatch os controles novamente, você pode associar a conta a uma nova política que habilite os controles. Como alternativa, você pode alterar a conta para autogerenciada e ativar cada CloudWatch controle na conta.
- As políticas de configuração entram em vigor na sua região inicial e em todas as regiões vinculadas: uma política de configuração afeta todas as contas associadas na região inicial e em todas as regiões vinculadas. Você não pode criar uma política de configuração que entre em vigor somente a algumas dessas regiões e não a outras. A exceção a isso são os controles que envolvem recursos globais.

  As regiões que AWS foram introduzidas em ou após 20 de março de 2019 são conhecidas como regiões opcionais. Você deve habilitar essa região para uma conta antes que uma política de configuração entre em vigor nela. A conta de gerenciamento do Organizations pode habilitar regiões de adesão para uma conta-membro. Para obter instruções sobre como ativar regiões opcionais, consulte Especificar qual Regiões da AWS conta pode ser usada no Guia de referência de gerenciamento de AWS contas.

  Se a sua política configurar um controle que não esteja disponível na região inicial ou em uma ou mais regiões vinculadas, o Security Hub ignorará a configuração do controle nas regiões indisponíveis, mas aplicará a configuração nas regiões em que o controle estiver disponível.

- Políticas de configuração são recursos: como recurso, uma política de configuração tem um nome do recurso da Amazon (ARN) e um identificador universalmente exclusivo (UUID). O ARN usa o formato a seguir: `arn:partition:securityhub:region:delegated administrator account ID:configuration-policy/configuration policy UUID`. Uma configuração autogerenciada não tem ARN nem UUID. O identificador de uma configuração autogerenciada é `SELF_MANAGED_SECURITY_HUB`.

Tipos de políticas de configuração

Cada política de configuração especifica as configurações a seguir:

- Habilitar ou desabilitar o Security Hub.
- Habilitar um ou mais padrões de segurança.
- Indicar quais controles de segurança estão habilitados dentre todos os padrões habilitados. É possível fazer isso fornecendo uma lista de controles específicos que devem ser habilitados, e o Security Hub desabilitará todos os outros controles, incluindo novos controles quando eles forem lançados. De forma alternativa, é possível fornecer uma lista de controles específicos que devem ser desabilitados, e o Security Hub habilitará todos os outros controles, incluindo novos controles quando eles forem lançados.
- Opcionalmente, personalize os parâmetros para selecionar controles habilitados dentre os padrões habilitados.

As políticas de configuração central não incluem as configurações do AWS Config gravador. Você deve habilitar AWS Config e ativar separadamente a gravação dos recursos necessários para que o Security Hub gere descobertas de controle. Para ter mais informações, consulte Configurando AWS Config.

Se você usar a configuração central, o Security Hub desativará automaticamente os controles que envolvem recursos globais em todas as regiões, exceto na região de origem. Outros controles que você escolhe ativar por meio de uma política de configuração são habilitados em todas as regiões em que estão disponíveis. Para limitar as descobertas desses controles a apenas uma região, você pode atualizar as configurações do AWS Config gravador e desativar a gravação global de recursos em todas as regiões, exceto na região de origem. Ao usar a configuração central, você não tem cobertura para um controle que não está disponível na região de origem e em nenhuma das regiões vinculadas. Para obter uma lista de controles que envolvem recursos globais, consulteControles que lidam com recursos globais.

Política de configuração recomendada

Ao criar uma política de configuração pela primeira vez no console do Security Hub, você tem a opção de escolher a política recomendada do Security Hub.

A política recomendada ativa o Security Hub, o padrão AWS Foundational Security Best Practices (FSBP) e todos os controles FSBP novos e existentes. Os controles que aceitam parâmetros usam os valores padrão. A política recomendada se aplica à raiz (todas as contas e OUs, novas e existentes). Depois de criar a política recomendada para sua organização, é possível modificá-la a partir da conta de administrador delegado. Por exemplo, é possível habilitar padrões ou controles adicionais ou desabilitar controles de FSBP específicos. Para obter instruções sobre como modificar uma política de configuração, consulte Atualização das políticas de configuração do Security Hub.

Política de configuração personalizada

Em vez da política recomendada, o administrador delegado pode criar até 20 políticas de configuração personalizadas. É possível associar uma única política personalizada a toda a sua organização ou políticas personalizadas diferentes a contas e OUs diferentes. Para uma política de configuração personalizada, você especifica as configurações desejadas. Por exemplo, é possível criar uma política personalizada que habilite o FSBP, o Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 e todos os controles nesses padrões, exceto os controles do Amazon Redshift. O nível de granularidade que você usa nas políticas de configuração personalizadas depende do escopo pretendido da cobertura de segurança em toda a organização.

> **Note**
>
> Você não pode associar uma política de configuração que desabilite o Security Hub à conta de administrador delegado. Essa política pode ser associada a outras contas, mas ignorará a associação com o administrador delegado. A conta de administrador delegado retém sua configuração atual.

Depois de criar uma política de configuração personalizada, é possível mudar para a política de configuração recomendada atualizando sua política de configuração para refletir a configuração recomendada. Entretanto, você não vê a opção de criar a política de configuração recomendada no console do Security Hub após a criação da primeira política.

Associação de políticas por meio de aplicação e herança

Quando você faz a adesão à configuração central pela primeira vez, sua organização não tem associações e se comporta da mesma forma que antes da adesão. O administrador delegado pode então estabelecer associações entre uma política de configuração ou um comportamento autogerenciado e contas, OUs ou a raiz. As associações podem ser estabelecidas por meio de aplicação ou herança.

A partir da conta de administrador delegado, é possível aplicar diretamente uma política de configuração a uma conta, OU ou raiz. Como alternativa, o administrador delegado pode aplicar diretamente uma designação autogerenciada a uma conta, UO ou à raiz.

Na ausência de aplicação direta, uma conta ou OU herda as configurações do pai mais próximo que tem uma política de configuração ou comportamento autogerenciado. Se o pai mais próximo estiver associado a uma política de configuração, o filho herdará essa política e poderá ser configurado somente pelo administrador delegado da região inicial. Se o pai mais próximo for autogerenciado, o filho herda o comportamento autogerenciado e poderá especificar suas próprias configurações em cada um. Região da AWS

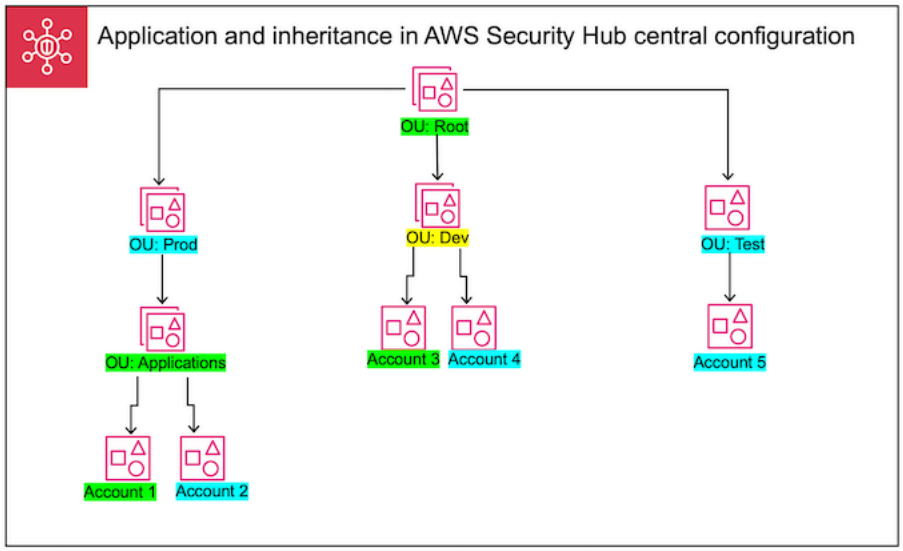
A aplicação tem precedência sobre a herança. Em outras palavras, a herança não substitui uma política de configuração ou uma designação autogerenciada que o administrador delegado tenha aplicado diretamente a uma conta ou UO.

Se você aplicar diretamente uma política de configuração a uma conta autogerenciada, a política substituirá a designação autogerenciada. A conta é gerenciada centralmente e adota as configurações refletidas na política de configuração.

Recomendamos aplicar diretamente uma política de configuração à raiz. Se você aplicar uma política à raiz, as novas contas que ingressarem na sua organização herdarão automaticamente a política da raiz, a menos que você as associe a uma política diferente ou as designe como autogerenciadas.

Somente uma política de configuração pode ser associada a uma conta ou OU em um determinado momento, seja por meio de aplicação ou herança. Isso foi projetado para evitar configurações conflitantes.

O diagrama a seguir ilustra como a aplicação de políticas e a herança funcionam na configuração central.



Neste exemplo, um nó destacado em verde tem uma política de configuração que foi aplicada a ele. Um nó destacado em azul não tem nenhuma política de configuração aplicada a ele. Um nó destacado em amarelo foi designado como autogerenciado. Cada conta e UO usam a configuração a seguir:

- OU:Raiz (verde): essa OU usa a política de configuração que foi aplicada a ela.
- OU:Prod (azul): essa OU herda a política de configuração de OU:Raiz.
- OU:Aplicações (verde): essa OU usa a política de configuração que foi aplicada a ela.
- Conta 1 (verde): essa conta usa a política de configuração que foi aplicada a ela.
- Conta 2 (azul): essa conta herda a política de configuração de OU:Aplicações.
- OU:Desenv (amarelo): essa OU é autogerenciada.
- Conta 3 (verde): essa conta usa a política de configuração que foi aplicada a ela.
- Conta 4 (azul): essa conta herda o comportamento autogerenciado de OU:Desenv.
- OU:Teste (azul): essa conta herda a política de configuração de OU:Raiz.
- Conta 5 (azul): essa conta herda a política de configuração de OU:Raiz, pois seu pai imediato, OU:Teste, não está associado a uma política de configuração.

Testes de uma política de configuração

Para testar o efeito de uma política de configuração, é possível associá-la a uma única conta ou OU antes de associá-la mais amplamente por toda a organização.

Para testar uma política de configuração

1. Crie uma política de configuração personalizada, mas não a aplique a nenhuma conta. Verifique se as configurações especificadas para habilitação, padrões e controles do Security Hub estão corretas.
2. Aplique a política de configuração a uma conta de teste ou OU que não tenha contas ou OUs filhas.
3. Verifique se a conta de teste ou OU usa a política de configuração da forma esperada em sua região inicial e em todas as regiões vinculadas. Você também pode verificar se todas as outras contas e OUs da sua organização permanecem autogerenciadas e podem alterar suas próprias configurações em cada região.

Depois de testar uma política de configuração em uma única conta ou OU, será possível associá-la a outras contas e OUs. Para obter instruções sobre a criação e associação de políticas, consulte Criação e associação de políticas de configuração do Security Hub. Os filhos das contas aplicadas herdam a política, a menos que sejam autogerenciados ou que uma política de configuração diferente se aplique a eles. Você também pode editar suas políticas de configuração e criar políticas de configuração adicionais conforme necessário.

Criação e associação de políticas de configuração do Security Hub

A conta de administrador delegado pode criar políticas de AWS Security Hub configuração e associá-las às contas da organização, às unidades organizacionais (OUs) ou à raiz. Você também pode associar uma configuração autogerenciada a contas, OUs ou à raiz.

Se essa for a primeira vez que você está criando uma política de configuração, é recomendável analisar primeiro Como as políticas de configuração do Security Hub funcionam.

Escolha seu método de acesso preferido e siga as etapas para criar e associar uma política de configuração ou configuração autogerenciada. Ao usar o console do Security Hub, você pode associar uma configuração a várias contas ou OUs ao mesmo tempo. Ao usar a API do Security Hub ou AWS CLI, você pode associar uma configuração a somente uma conta ou OU em cada solicitação.

> **Note**
>
> Se você usar a configuração central, o Security Hub desativará automaticamente os controles que envolvem recursos globais em todas as regiões, exceto na região de origem.

Outros controles que você escolhe ativar por meio de uma política de configuração são habilitados em todas as regiões em que estão disponíveis. Para limitar as descobertas desses controles a apenas uma região, você pode atualizar as configurações do AWS Config gravador e desativar a gravação global de recursos em todas as regiões, exceto na região de origem. Ao usar a configuração central, você não tem cobertura para um controle que não está disponível na região de origem e em nenhuma das regiões vinculadas. Para obter uma lista de controles que envolvem recursos globais, consulteControles que lidam com recursos globais.

Security Hub console

Para criar e associar políticas de configuração

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

   Faça login usando as credenciais da conta do administrador delegado do Security Hub na região inicial.
2. No painel de navegação, escolha Configuração e a guia Políticas. Em seguida, selecione Criar política.
3. Na página Configurar organização, se for a primeira vez que você cria uma política de configuração, você verá três opções em Tipo de configuração. Se você já criou pelo menos uma política de configuração, verá somente a opção Política personalizada.

   - Escolha Usar a configuração AWS recomendada do Security Hub em toda a minha organização para usar nossa política recomendada. A política recomendada ativa o Security Hub em todas as contas da organização, ativa o padrão AWS Foundational Security Best Practices (FSBP) e ativa todos os controles FSBP novos e existentes. Os controles usam valores de parâmetros padrão.
   - Escolha Ainda não estou pronto para configurar para criar uma política de configuração mais tarde.
   - Escolha Política personalizada para criar uma política de configuração personalizada. Especifique se deseja habilitar ou desabilitar o Security Hub, quais padrões habilitar e quais controles habilitar em todos esses padrões. Opcionalmente, especifique valores de parâmetros personalizados para um ou mais controles habilitados que ofereçam suporte a parâmetros personalizados.

4. Na seção Contas, escolha a quais contas de destino, OUs ou a raiz você deseja que sua política de configuração se aplique.

   - Escolha Todas as contas se quiser aplicar a política de configuração à raiz. Isso inclui todas as contas e OUs da organização que não tenham outra política aplicada ou herdada.
   - Escolha Contas específicas se quiser aplicar a política de configuração a contas ou OUs específicas. Insira os IDs da conta ou selecione as contas e OUs na estrutura da organização. Você pode aplicar a política a um máximo de 15 contas ou a uma OU contendo no máximo 15 contas. Para especificar um número maior, edite sua política após a criação e aplique-a a contas adicionais.
   - Escolha Somente o administrador delegado para aplicar a política de configuração à conta atual do administrador delegado.

5. Escolha Próximo.
6. Na página Revisar e aplicar, revise os detalhes da configuração. Em seguida, escolha Criar política e aplicar. Na sua região inicial e em todas as regiões vinculadas, essa ação substituirá as configurações existentes das contas associadas a essa política de configuração. As contas podem ser associadas à política de configuração por meio de aplicação direta ou herança de um nó pai. As contas e OUs filhas dos destinos aplicados herdarão automaticamente essa política de configuração, a menos que sejam especificamente excluídas, autogerenciadas ou usem uma política de configuração diferente.

Security Hub API

Para criar e associar políticas de configuração

1. Invoque a API CreateConfigurationPolicy a partir da conta de administrador delegado do Security Hub na região inicial.
2. Em `Name`, insira um nome exclusivo para a política de configuração. Opcionalmente, em `Description`, forneça uma descrição para a política de configuração.
3. No campo `ServiceEnabled`, especifique se você deseja que o Security Hub seja habilitado ou desabilitado nesta política de configuração.
4. No campo `EnabledStandardIdentifiers`, especifique quais padrões do Security Hub você deseja habilitar nesta política de configuração.
5. No objeto `SecurityControlsConfiguration`, especifique quais controles você deseja habilitar ou desabilitar nessa política de configuração. Escolher

`EnabledSecurityControlIdentifiers` significa que os controles especificados serão habilitados. Outros controles que façam parte de seus padrões habilitados (incluindo controles recém-lançados) serão desabilitados. Escolher `DisabledSecurityControlIdentifiers` significa que os controles especificados serão desabilitados. Outros controles que façam parte de seus padrões habilitados (incluindo controles recém-lançados) serão habilitados.

6. Opcionalmente, no campo `SecurityControlCustomParameters`, especifique os controles habilitados para os quais você deseja personalizar os parâmetros. Forneça `CUSTOM` para o campo `ValueType` e o valor do parâmetro personalizado para o campo `Value`. O valor deve ser do tipo de dados correto e estar dentro dos intervalos válidos especificados pelo Security Hub. Somente controles selecionados oferecem suporte a valores de parâmetros personalizados. Para ter mais informações, consulte Parâmetros de controle personalizados.
7. Para aplicar sua política de configuração a contas ou OUs, invoque a API StartConfigurationPolicyAssociation da conta de administrador delegado do Security Hub na região inicial.
8. Para o `ConfigurationPolicyIdentifier` campo, forneça o Amazon Resource Name (ARN) ou o identificador universalmente exclusivo (UUID) da política. O ARN e o UUID são retornados pela API. `CreateConfigurationPolicy` Para uma configuração autogerenciada, o `ConfigurationPolicyIdentifier` campo é igual a. `SELF_MANAGED_SECURITY_HUB`
9. No campo `Target`, forneça o ID da OU, da conta ou da raiz à qual você deseja que essa política de configuração se aplique. Você só pode fornecer um destino em cada solicitação de API. As contas e UOs filhas do destino selecionado herdarão automaticamente esta política de configuração, a menos que sejam autogerenciadas ou usem uma política de configuração diferente.

Exemplo de solicitação de API para criar uma política de configuração:

```
{
    "Name": "SampleConfigurationPolicy",
    "Description": "Configuration policy for production accounts",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
```

```
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

Exemplo de solicitação de API para associar uma política de configuração:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}
```

AWS CLI

Para criar e associar políticas de configuração

1. Execute o comando create-configuration-policy a partir da conta de administrador delegado do Security Hub na região inicial.

2. Em `name`, insira um nome exclusivo para a política de configuração. Opcionalmente, em `description`, forneça uma descrição para a política de configuração.
3. No campo `ServiceEnabled`, especifique se você deseja que o Security Hub seja habilitado ou desabilitado nesta política de configuração.
4. No campo `EnabledStandardIdentifiers`, especifique quais padrões do Security Hub você deseja habilitar nesta política de configuração.
5. No campo `SecurityControlsConfiguration`, especifique quais controles você deseja habilitar ou desabilitar nessa política de configuração. Escolher `EnabledSecurityControlIdentifiers` significa que os controles especificados serão habilitados. Outros controles que façam parte de seus padrões habilitados (incluindo controles recém-lançados) serão desabilitados. Escolher `DisabledSecurityControlIdentifiers` significa que os controles especificados serão desabilitados. Outros controles que se apliquem aos seus padrões habilitados (incluindo controles recém-lançados) serão habilitados.
6. Opcionalmente, no campo `SecurityControlCustomParameters`, especifique os controles habilitados para os quais você deseja personalizar os parâmetros. Forneça `CUSTOM` para o campo `ValueType` e o valor do parâmetro personalizado para o campo `Value`. O valor deve ser do tipo de dados correto e estar dentro dos intervalos válidos especificados pelo Security Hub. Somente controles selecionados oferecem suporte a valores de parâmetros personalizados. Para ter mais informações, consulte Parâmetros de controle personalizados.
7. Para aplicar sua política de configuração a contas ou OUs, execute o comando start-configuration-policy-association da conta de administrador delegado do Security Hub na região inicial.
8. No campo `configuration-policy-identifier`, forneça o nome do recurso da Amazon (ARN) ou o ID da política de configuração. Esse ARN e ID são retornados pelo comando `create-configuration-policy`.
9. No campo `target`, forneça o ID da OU, da conta ou da raiz à qual você deseja que essa política de configuração se aplique. Você só pode fornecer um destino a cada vez que você executa o comando. Os filhos do destino selecionado herdarão automaticamente esta política de configuração, a menos que sejam autogerenciadas ou usem uma política de configuração diferente.

Exemplo de comando para criar uma política de configuração:

```
aws securityhub --region us-east-1 create-configuration-policy \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}'
```

Exemplo de comando para associar uma política de configuração:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}'
```

A API `StartConfigurationPolicyAssociation` retorna um campo chamado `AssociationStatus`. Esse campo informa se uma associação de política está pendente ou em um estado de sucesso ou fracasso. Pode demorar até 24 horas para que o status mude de `PENDING` para `SUCCESS` ou `FAILURE`. Para obter mais informações sobre status de associações, consulte Status da associação de uma configuração.

Exibição das políticas de configuração do Security Hub

A conta de administrador delegado pode visualizar as políticas de configuração do AWS Security Hub de uma organização e seus detalhes.

Escolha seu método preferido e siga as etapas para visualizar suas políticas de configuração.

Console

Para visualizar as políticas de configuração

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.

Faça login usando as credenciais da conta do administrador delegado do Security Hub na região inicial.

2. No painel de navegação, escolha Configurações e Configuração.
3. Escolha a guia Políticas para ver uma visão geral de suas políticas de configuração.
4. Selecione uma política de configuração e escolha Exibir detalhes para ver detalhes adicionais sobre ela.

API

Para visualizar as políticas de configuração

Para ver uma lista resumida de todas as suas políticas de configuração, invoque a API `ListConfigurationPolicies` da conta de administrador delegado do Security Hub em sua região inicial. É possível fornecer parâmetros de paginação opcionais

Exemplo de solicitação de API:

```
{
    "MaxResults": 5,
    "NextToken": "U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf"
}
```

Para ver detalhes sobre uma política de configuração específica, invoque a API `GetConfigurationPolicy` da conta de administrador delegado do Security Hub em sua região inicial. Forneça o nome do recurso da Amazon (ARN) ou o ID da política de configuração cujos detalhes você deseja visualizar.

Exemplo de solicitação de API:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Para ver uma lista resumida de todas as suas políticas de configuração e suas associações, invoque a API `ListConfigurationPolicyAssociations` da conta de administrador

delegado do Security Hub em sua região inicial. Opcionalmente, é possível fornecer parâmetros de paginação ou filtrar os resultados por um ID de política específica, tipo de associação ou status de associação.

Exemplo de solicitação de API:

```
{
    "AssociationType": "APPLIED"
}
```

Para visualizar as associações para uma conta, OU ou raiz específica, invoque a API `GetConfigurationPolicyAssociation` ou`BatchGetConfigurationPolicyAssociations` a partir da conta de administrador delegado do Security Hub em sua região inicial. Em `Target`, forneça o número da conta, ID da OU ou ID da raiz.

```
{
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

Para visualizar as políticas de configuração

Para ver uma lista resumida de todas as suas políticas de configuração, execute o comando `list-configuration-policies` na conta de administrador delegado do Security Hub em sua região inicial.

Exemplo de comando:

```
aws securityhub --region us-east-1 list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf
```

Para ver detalhes sobre uma política de configuração específica, execute o comando `get-configuration-policy` da conta de administrador delegado do Security Hub em sua região inicial. Forneça o nome do recurso da Amazon (ARN) ou o ID da política de configuração cujos detalhes você deseja visualizar.

```
aws securityhub --region us-east-1 get-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Para ver uma lista resumida de todas as suas políticas de configuração e suas associações de conta, execute o comando `list-configuration-policy-associations` na conta de administrador delegado do Security Hub em sua região inicial. Opcionalmente, é possível fornecer parâmetros de paginação ou filtrar os resultados por um ID de política específica, tipo de associação ou status de associação.

```
aws securityhub --region us-east-1 list-configuration-policy-associations \
--association-type "APPLIED"
```

Para ver as associações de uma conta específica, execute o comando `get-configuration-policy-association` ou `batch-get-configuration-policy-associations` na conta de administrador delegado do Security Hub em sua região inicial. Em `target`, forneça o número da conta, ID da OU ou ID da raiz.

```
aws securityhub --region us-east-1 get-configuration-policy-association \
--target '{"AccountId": "123456789012"}'
```

Status da associação de uma configuração

As operações a seguir da API da configuração central retornam um campo chamado `AssociationStatus`:

- `BatchGetConfigurationPolicyAssociations`
- `GetConfigurationPolicyAssociation`
- `ListConfigurationPolicyAssociations`
- `StartConfigurationPolicyAssociation`

Esse campo é retornado quando a configuração subjacente é uma política de configuração e quando é um comportamento autogerenciado.

O valor de `AssociationStatus` indica se uma associação de política está pendente ou em estado de êxito ou fracasso. Pode demorar até 24 horas para que o status mude de `PENDING` para `SUCCESS` ou `FAILURE`. O status da associação de uma OU principal ou da raiz depende do status de seus filhos. Se o status de associação de todos os filhos for `SUCCESS`, o status de associação dos pais será `SUCCESS`. Se o status de associação de um ou mais filhos for `FAILED`, o status de associação dos pais será `FAILED`.

O valor de `AssociationStatus` também depende de todas as regiões. Se a associação obtiver êxito na região inicial e em todas as regiões vinculadas, o valor de `AssociationStatus` será `SUCCESS`. Se a associação falhar em uma ou mais dessas regiões, o valor de `AssociationStatus` será `FAILED`.

O comportamento a seguir também afeta o valor de `AssociationStatus`:

- Se o destino for uma OU pai ou a raiz, ela terá um `AssociationStatus` de `SUCCESS` ou `FAILED` somente quando todos os filhos tiverem um status `SUCCESS` ou `FAILED`. Se o status de associação de uma conta secundária ou OU mudar (por exemplo, quando uma região vinculada for adicionada ou removida) depois que você associar o pai a uma configuração pela primeira vez, a alteração não atualizará o status de associação do pai, a menos que você invoque a API `StartConfigurationPolicyAssociation` novamente.
- Se o destino for uma conta, ela terá um `AssociationStatus` de `SUCCESS` ou `FAILED` somente se a associação tiver um resultado de `SUCCESS` ou `FAILED` na região inicial e em todas as regiões vinculadas. Se o status de associação de uma conta de destino mudar (por exemplo, quando uma região vinculada for adicionada ou removida) depois que você a associar pela primeira vez a uma configuração, seu status de associação será atualizado. Entretanto, a alteração não atualiza o status de associação do pai, a menos que você invoque a API `StartConfigurationPolicyAssociation` novamente.

Se você adicionar uma nova região vinculada, o Security Hub replicará suas associações existentes que estiverem em um estado `PENDING`, `SUCCESS` ou `FAILED` na nova região.

Motivos comuns de falha de associação

Uma associação de política de configuração pode falhar pelos motivos comuns a seguir:

- A conta de gerenciamento do Organizations não é um membro: se você quiser associar uma política de configuração à conta de gerenciamento do Organizations, essa conta já deve ter o Security Hub habilitado. Isso torna a conta de gerenciamento uma conta-membro na organização.

- A AWS Config não está habilitada ou configurada corretamente: para habilitar padrões em uma política de configuração, a AWS Config deve estar habilitada e configurada para registrar recursos relevantes.
- É necessário associar a partir da conta de administrador delegado: você só pode associar uma política a contas e OUs de destino quando estiver conectado à conta de administrador delegado.
- É necessário associar a partir da região inicial: você só pode associar uma política às contas e OUs de destino quando estiver conectado à região inicial.
- Região de adesão não habilitada: a associação de políticas falhará para uma conta-membro ou OU em uma região vinculada se for uma região de adesão que o administrador delegado não tenha habilitado. É possível tentar novamente depois de habilitar a região a partir da conta de administrador delegado.
- Conta-membro suspensa: a associação de políticas falhará se você tentar associar uma política a uma conta-membro suspensa.

Atualização das políticas de configuração do Security Hub

A conta de administrador delegado pode atualizar as políticas AWS Security Hub de configuração conforme necessário. O administrador delegado pode atualizar as configurações da política, as contas ou OUs às quais uma política está associada, ou ambas. Quando as configurações da política são atualizadas, as contas associadas à política de configuração começarão automaticamente a usar a política atualizada.

Da mesma forma que quando você criou a política de configuração, é possível atualizar as configurações de política a seguir:

- Habilitar ou desabilitar o Security Hub.
- Habilitar um ou mais padrões de segurança.
- Indicar quais controles de segurança estão habilitados dentre todos os padrões habilitados. É possível fazer isso fornecendo uma lista de controles específicos que devem ser habilitados, e o Security Hub desabilitará todos os outros controles, incluindo novos controles quando eles forem lançados. De forma alternativa, é possível fornecer uma lista de controles específicos que devem ser desabilitados, e o Security Hub habilitará todos os outros controles, incluindo novos controles quando eles forem lançados.
- Opcionalmente, personalize os parâmetros para selecionar controles habilitados dentre os padrões habilitados.

Escolha seu método preferido e siga as etapas para atualizar uma política de configuração.

Se você usar a configuração central, o Security Hub desativará automaticamente os controles que envolvem recursos globais em todas as regiões, exceto na região de origem. Outros controles que você escolhe ativar por meio de uma política de configuração são habilitados em todas as regiões em que estão disponíveis. Para limitar as descobertas desses controles a apenas uma região, você pode atualizar as configurações do AWS Config gravador e desativar a gravação global de recursos em todas as regiões, exceto na região de origem. Ao usar a configuração central, você não tem cobertura para um controle que não está disponível na região de origem e em nenhuma das regiões vinculadas. Para obter uma lista de controles que envolvem recursos globais, consulte Controles que lidam com recursos globais.

Console

Para atualizar políticas de configuração

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

   Faça login usando as credenciais da conta do administrador delegado do Security Hub na região inicial.
2. No painel de navegação, escolha Configurações e Configuração.
3. Escolha a guia Políticas.
4. Selecione a política de configuração que deseja editar e escolha Editar. Se desejar, edite as configurações da política. Deixe esta seção como está se desejar manter as configurações de políticas inalteradas.
5. Escolha Avançar. Se desejar, edite as associações de políticas. Deixe esta seção como está se desejar manter as associações de políticas inalteradas.
6. Escolha Próximo.
7. Revise suas alterações e escolha Salvar e aplicar. Na sua região inicial e em todas as regiões vinculadas, essa ação substituirá as configurações existentes das contas associadas a essa política de configuração. As contas podem ser associadas a uma política de configuração por meio de aplicação direta ou herança de um nó pai.

API

Para atualizar políticas de configuração

1. Para atualizar as configurações em uma política de configuração, invoque a API UpdateConfigurationPolicy da conta de administrador delegado do Security Hub na região inicial.
2. Forneça o nome do recurso da Amazon (ARN) ou o ID da política de configuração que deseja atualizar.
3. Forneça valores atualizados para os campos sob `ConfigurationPolicy`. Opcionalmente, também é possível fornecer um motivo para a atualização.
4. Para adicionar novas associações a essa política de configuração, invoque a API StartConfigurationPolicyAssociation da conta de administrador delegado do Security Hub na região inicial. Para remover uma ou mais das associações atuais, invoque a API StartConfigurationPolicyDisassociation a partir da conta de administrador delegado do Security Hub na região inicial.
5. No campo `ConfigurationPolicyIdentifier`, forneça o ARN ou o ID da política de configuração cujas associações você deseja atualizar.
6. No campo `Target`, forneça o ID das contas, OUs da raiz que você deseja associar ou desassociar. Essa ação substitui associações de políticas anteriores para as OUs ou contas especificadas.

> **Note**
>
> Quando você invoca a API `UpdateConfigurationPolicy`, o Security Hub executa uma substituição completa da lista para os campos `EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiers`, `DisabledSecurityControlIdentifiers` e `SecurityControlCustomParameters`. Sempre que você invocar essa API, forneça a lista completa dos padrões que você deseja habilitar e a lista completa dos controles para os quais você deseja habilitar ou desabilitar e personalizar os parâmetros.

Exemplo de solicitação de API para atualizar uma política de configuração:

```
{
```

```
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Description": "Updated configuration policy",
    "UpdatedReason": "Disabling CloudWatch.1",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2",
                    "CloudWatch.1"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

AWS CLI

Para atualizar políticas de configuração

1. Para atualizar as configurações em uma política de configuração, execute o comando update-configuration-policy a partir da conta de administrador delegado do Security Hub na região inicial.
2. Forneça o nome do recurso da Amazon (ARN) ou o ID da política de configuração que deseja atualizar.
3. Forneça valores atualizados para os campos sob `configuration-policy`. Opcionalmente, também é possível fornecer um motivo para a atualização.
4. Para adicionar novas associações a essa política de configuração, execute o comando start-configuration-policy-association a partir da conta de administrador delegado do Security Hub na região inicial. Para remover uma ou mais das associações atuais, execute o comando start-configuration-policy-disassociation a partir da conta de administrador delegado do Security Hub na região inicial.
5. No campo `configuration-policy-identifier`, forneça o ARN ou o ID da política de configuração cujas associações você deseja atualizar.
6. No campo `target`, forneça o ID das contas, OUs da raiz que você deseja associar ou desassociar. Essa ação substitui associações de políticas anteriores para as OUs ou contas especificadas.

> **Note**
>
> Quando você executa o comando `update-configuration-policy`, o Security Hub executa uma substituição completa da lista para os campos `EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiers`, `DisabledSecurityControlIdentifiers` e `SecurityControlCustomParameters`. Sempre que você executar esse comando, forneça a lista completa dos padrões que você deseja habilitar e a lista completa dos controles para os quais você deseja habilitar ou desabilitar e personalizar os parâmetros.

Exemplo de comando para atualizar uma política de configuração:

```
aws securityhub update-configuration-policy \
```

```
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--description "Updated configuration policy" \
--updated-reason "Disabling CloudWatch.1" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2","CloudWatch.1"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}}'
```

A API `StartConfigurationPolicyAssociation` retorna um campo chamado `AssociationStatus`. Esse campo informa se uma associação de política está pendente ou em um estado de sucesso ou fracasso. Pode demorar até 24 horas para que o status mude de `PENDING` para `SUCCESS` ou `FAILURE`. Para obter mais informações sobre status de associações, consulte Status da associação de uma configuração.

Exclusão e desassociação de políticas de configuração do Security Hub

A conta de administrador delegado pode excluir uma política de configuração do AWS Security Hub. Como alternativa, a conta de administrador delegado pode reter a política de configuração, mas desassociá-la de contas ou unidades organizacionais (OUs) específicas.

As seções a seguir explicam ambas essas opções.

Exclusão de políticas de configuração

Quando você exclui uma política de configuração, ela deixa de existir para sua organização. As contas de destino, OUs e a raiz da organização não poderão mais usar a política de configuração. Os destinos associados a uma política de configuração excluída herdam a política de configuração do pai mais próximo ou se tornam autogerenciados se o pai mais próximo for autogerenciado. Se quiser que um destino use uma configuração diferente, é possível associar o destino a uma nova política de configuração. Para obter mais informações, consulte Criação e associação de políticas de configuração do Security Hub.

Recomendamos criar e associar pelo menos uma política de configuração à sua organização para fornecer cobertura de segurança adequada.

Antes de excluir uma política de configuração, você deverá desassociar a política das contas, OUs ou da raiz à qual ela se aplica atualmente.

Escolha seu método preferido e siga as etapas para excluir uma política de configuração.

Console

Para excluir uma política de configuração

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.

   Faça login usando as credenciais da conta do administrador delegado do Security Hub na região inicial.
2. No painel de navegação, escolha Configurações e Configuração.
3. Escolha a guia Políticas. Selecione a política de configuração que você deseja excluir e, em seguida, escolha Excluir. Se a política de configuração ainda estiver associada a contas ou OUs, você será solicitado a primeiro desassociar a política desses destinos antes de excluí-la.
4. Revise a mensagem de confirmação. Insira **`confirm`** e escolha Excluir.

API

Para excluir uma política de configuração

Invoque a API DeleteConfigurationPolicy a partir da conta de administrador delegado do Security Hub na região inicial.

Forneça o nome do recurso da Amazon (ARN) ou o ID da política de configuração que deseja excluir. Se você receber um erro `ConflictException`, a política de configuração ainda se aplicará às contas ou OUs em sua organização. Para resolver o erro, desassocie a política de configuração dessas contas ou OUs antes de tentar excluí-la.

Exemplo de solicitação de API para excluir uma política de configuração:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

```
}
```

AWS CLI

Para excluir uma política de configuração

Execute o comando delete-configuration-policy a partir da conta de administrador delegado do Security Hub na região inicial.

Forneça o nome do recurso da Amazon (ARN) ou o ID da política de configuração que deseja excluir. Se você receber um erro `ConflictException`, a política de configuração ainda se aplicará às contas ou OUs em sua organização. Para resolver o erro, desassocie a política de configuração dessas contas ou OUs antes de tentar excluí-la.

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Desassociação de uma configuração de contas e OUs

Na conta de administrador delegado, é possível desassociar uma conta de destino, OU ou a raiz de uma política de configuração que atualmente se aplica a ela ou de uma configuração autogerenciada. É possível desassociar um destino somente de uma configuração aplicada, não de uma configuração herdada. Para alterar uma configuração herdada, é possível aplicar uma política de configuração ou um comportamento autogerenciado à conta ou OU afetada. Você também pode aplicar uma nova política de configuração, que inclua as modificações desejadas, ao pai mais próximo.

A desassociação não exclui uma política de configuração. A política é retida em sua conta, para que você possa associá-la a outras metas em sua organização. Quando a desassociação é concluída, um destino afetado herda a política de configuração ou o comportamento autogerenciado do pai mais próximo. Se não houver uma configuração herdável, o destino reterá as configurações que tinha antes da desassociação, mas se tornará autogerenciado.

Escolha seu método preferido e siga as etapas para desassociar uma conta, UO ou ou a raiz de sua configuração atual.

Console

Para desassociar uma conta ou OU de sua configuração atual

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.

   Faça login usando as credenciais da conta do administrador delegado do Security Hub na região inicial.
2. No painel de navegação, escolha Configurações e Configuração.
3. Na guia Organizations, selecione a conta, a OU ou a raiz que você deseja desassociar da configuração atual. Selecione a opção Editar.
4. Na página Definir configuração, em Gerenciamento, escolha Política aplicada se quiser que o administrador delegado possa aplicar políticas diretamente ao destino. Escolha Herdada se desejar que o destino herde a configuração do pai mais próximo. Em qualquer um desses casos, o administrador delegado controlará as configurações do destino. Escolha Autogerenciado se desejar que a conta ou OU controle suas próprias configurações.
5. Depois de revisar suas alterações, escolha Avançar e Aplicar. Essa ação substituirá as configurações existentes de todas as contas ou OUs que estejam no escopo, caso essas configurações entrem em conflito com suas seleções atuais.

API

Para desassociar uma conta ou OU de sua configuração atual

1. Invoque a API StartConfigurationPolicyDisassociation a partir da conta de administrador delegado do Security Hub na região inicial.
2. Em `ConfigurationPolicyIdentifier`, forneça o nome do recurso da Amazon (ARN) ou o ID da política de configuração que deseja desassociar. Forneça `SELF_MANAGED_SECURITY_HUB` para esse campo, para desassociar o comportamento autogerenciado.
3. Em `Target`, forneça as contas, OUs ou a raiz que você deseja dissociar dessa política de configuração.

Exemplo de solicitação de API para desassociar uma política de configuração:

```
{
```

```
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

Para desassociar uma conta ou OU de sua configuração atual

1. Execute o comando start-configuration-policy-disassociation a partir da conta de administrador delegado do Security Hub na região inicial.
2. Em `configuration-policy-identifier`, forneça o nome do recurso da Amazon (ARN) ou o ID da política de configuração que deseja desassociar. Forneça `SELF_MANAGED_SECURITY_HUB` para esse campo, para desassociar o comportamento autogerenciado.
3. Em `target`, forneça as contas, OUs ou a raiz que você deseja dissociar dessa política de configuração.

Exemplo de comando para desassociar uma política de configuração:

```
aws securityhub --region us-east-1 start-configuration-policy-disassociation \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"RootId": "r-f6g7h8i9j0example"}'
```

A configuração central no contexto de um padrão ou controle

Você pode usar a configuração central na página Configuração do AWS Security Hub console ou no contexto de um padrão de segurança ou controle de segurança específico. O uso desse recurso em contexto permite configurar padrões e controles em toda a organização de forma integrada aos fluxos de trabalho existentes. Além disso, ao visualizar as descobertas, é possível descobrir quais padrões e controles são mais relevantes para seu ambiente e configurá-los ao mesmo tempo.

A configuração contextual está disponível somente no console do Security Hub. Programaticamente, você deve invocar a API UpdateConfigurationPolicy para alterar a forma como os padrões ou controles específicos são configurados em sua organização.

Configuração de um padrão de segurança em contexto

Siga as etapas para configurar um padrão de segurança em contexto por meio da configuração central.

Para configurar um padrão de segurança em contexto (somente console)

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

   Faça login usando as credenciais da conta do administrador delegado do Security Hub na região inicial.
2. No painel de navegação, escolha Padrões de segurança.
3. Para o padrão que você desejar configurar, escolha Configurar. Você também pode escolher um padrão específico e, em seguida, escolher Configurar na página de detalhes do padrão. O console lista suas políticas de configuração existentes do Security Hub (políticas de configuração) e o status desse padrão em cada uma.
4. Escolha as opções para habilitar ou desabilitar o padrão em cada política de configuração.
5. Depois de fazer suas alterações, escolha Avançar.
6. Revise suas alterações e escolha Aplicar. Essa ação afeta todas as contas e OUs associadas a uma política de configuração. Sua configuração entrará em vigor na região inicial e em todas as regiões vinculadas.

Configuração de um controle de segurança em contexto

Siga as etapas para configurar um controle de segurança em contexto por meio da configuração central.

Para configurar um controle de segurança em contexto (somente console)

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

   Faça login usando as credenciais da conta do administrador delegado do Security Hub na região inicial.
2. No painel de navegação, escolha Controles.
3. Escolha um controle específico e, em seguida, escolha Configurar. O console lista suas políticas de configuração atuais e o status desse controle em cada uma.

4. Escolha as opções para habilitar ou desabilitar o controle em cada política de configuração. Você também pode optar por personalizar os parâmetros de controle.
5. Depois de fazer suas alterações, escolha Avançar.
6. Revise suas alterações e escolha Aplicar. Essa ação afeta todas as contas e OUs associadas a uma política de configuração. Sua configuração entrará em vigor na região inicial e em todas as regiões vinculadas.

Interromper o uso da configuração central

Quando você para de usar a configuração central no AWS Security Hub, o administrador delegado perde a capacidade de configurar o Security Hub, os padrões de segurança e os controles de segurança em várias Contas da AWS unidades organizacionais (OUs) e Regiões da AWS. Em vez disso, as contas da organização devem definir a maioria de suas próprias configurações separadamente em cada região.

> **Important**
>
> Antes de poder interromper o uso da configuração central, você deve primeiro desassociar suas contas e OUs da configuração atual, seja uma política de configuração ou um comportamento autogerenciado.
> Antes de interromper o uso da configuração central, você também deverá excluir suas políticas de configuração.

Quando você interrompe a configuração central, as alterações a seguir ocorrem:

- O administrador delegado não pode mais criar políticas de configuração para a organização.
- As contas que tiveram uma política de configuração aplicada ou herdada retêm suas configurações atuais, mas se tornam autogerenciadas.
- Sua organização muda para a configuração local. Na configuração local, a maioria das configurações do Security Hub deve ser definida separadamente em cada conta da organização e região. O administrador delegado pode optar por habilitar automaticamente o Security Hub, os padrões de segurança padrão e todos os controles que fazem parte dos padrões padrão em novas contas da organização. Os padrões de segurança padrão são o Práticas Recomendadas de Segurança Básica (FSBP) da AWS e o Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Essas novas configurações entram em vigor somente na região atual, e

afetarão somente as novas contas da organização. O administrador delegado não pode alterar quais padrões são padrão. A configuração local não oferece suporte ao uso de políticas de configuração ou de configuração no nível de OU.

A identidade da conta de administrador delegado permanece a mesma quando você para de usar a configuração central. Sua região inicial e as regiões vinculadas também permanecem as mesmas (sua região inicial agora é chamada de região de agregação e pode ser usada para agregar descobertas).

Escolha seu método preferido e siga as etapas para parar de usar a configuração central e mudar para a configuração local.

Security Hub console

Para interromper o uso da configuração central

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.

   Faça login usando as credenciais da conta do administrador delegado do Security Hub na região inicial.
2. No painel de navegação, escolha Configurações e Configuração.
3. Na seção Visão geral, selecione Editar.
4. Na caixa Editar configuração da organização, escolha Configuração local. Se ainda não o fez, você será solicitado a desassociar e excluir suas políticas de configuração atuais antes de poder interromper a configuração central. As contas ou OUs designadas como autogerenciadas devem ser desassociadas de sua configuração autogerenciada. É possível fazer isso no console alterando o tipo de gerenciamento de cada conta autogerenciada ou OU para Gerenciado centralmente e Herdar da minha organização.
5. Opcionalmente, selecione as definições padrão da configuração local para novas contas da organização.
6. Selecione a opção Confirmar.

Security Hub API

Para interromper o uso da configuração central

1. Invoque a API UpdateOrganizationConfiguration.

2. Defina o campo `ConfigurationType` no objeto `OrganizationConfiguration` como `LOCAL`. A API retornará um erro se você tiver políticas de configuração ou associações de políticas existentes. Para desassociar uma política de configuração, invoque a API `StartConfigurationPolicyDisassociation`. Para excluir uma política de configuração, invoque a API `DeleteConfigurationPolicy`.
3. Se você desejar habilitar automaticamente o Security Hub nas novas contas da organização, defina o campo `AutoEnable` como `true`. Por padrão, o valor desse campo é `false`, e o Security Hub não é habilitado automaticamente nas novas contas da organização. Opcionalmente, se você desejar habilitar automaticamente os padrões de segurança padrão nas novas contas da organização, defina o campo `AutoEnableStandards` como `DEFAULT`. Esse é o valor padrão. Se você não desejar habilitar automaticamente os padrões de segurança padrão nas novas contas da organização, defina o campo `AutoEnableStandards` como `NONE`.

Exemplo de solicitação de API:

```
{
    "AutoEnable": true,
    "OrganizationConfiguration": {
        "ConfigurationType" : "LOCAL"
    }
}
```

AWS CLI

Para interromper o uso da configuração central

1. Execute o comando update-organization-configuration.
2. Defina o campo `ConfigurationType` no objeto `organization-configuration` como `LOCAL`. O comando retornará um erro se você tiver políticas de configuração ou associações de políticas existentes. Para desassociar uma política de configuração, execute o comando `start-configuration-policy-disassociation`. Para excluir uma política de configuração, execute o comando `delete-configuration-policy`.
3. Se você desejar habilitar automaticamente o Security Hub nas novas contas da organização, inclua o parâmetro `auto-enable`. Por padrão, o valor desse parâmetro é `no-auto-enable`, e o Security Hub não é habilitado automaticamente nas novas contas da

organização. Opcionalmente, se você desejar habilitar automaticamente os padrões de segurança padrão nas novas contas da organização, defina o campo `auto-enable-standards` como `DEFAULT`. Esse é o valor padrão. Se você não desejar habilitar automaticamente os padrões de segurança padrão nas novas contas da organização, defina o campo `auto-enable-standards` como `NONE`.

```
aws securityhub --region us-east-1 update-organization-configuration \
--auto-enable \
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

Gerenciar contas de administrador e membro

Se o seu ambiente da AWS tiver várias contas, será possível tratar as contas que usam o AWS Security Hub como contas-membro e associá-las a uma única conta de administrador. O administrador pode monitorar sua postura geral de segurança e realizar ad ações permitidas nas contas dos membros. O administrador também pode realizar várias tarefas de gerenciamento e administração de contas em grande escala, como monitorar os custos de uso estimados e avaliar as cotas da conta.

É possível associar contas-membro a um administrador de duas maneiras: integrando o Security Hub com o AWS Organizations ou enviando e aceitando manualmente os convites de associação de membros no Security Hub.

Gerenciando contas com o AWS Organizations

O AWS Organizations é um serviço global de gerenciamento de contas que permite aos administradores da AWS consolidar e gerenciar várias Contas da AWS. Ele fornece os atributos de faturamento consolidado e gerenciamento de contas, projetados para atender às necessidades orçamentárias, de segurança e de conformidade. Ele é oferecido sem custo adicional e se integra a vários Serviços da AWS, incluindo o AWS Security Hub, o Amazon GuardDuty e o Amazon Macie. Para obter mais informações, consulte o AWS OrganizationsGuia do Usuário.

Quando você integra o Security Hub com o AWS Organizations, a conta de gerenciamento do Organizations designa um administrador delegado do Security Hub. O Security Hub é habilitado automaticamente na conta de administrador delegado na Região da AWS onde ele foi designado.

Depois de designar um administrador delegado, recomendamos gerenciar contas no Security Hub com a configuração central. Essa é a maneira mais eficiente de personalizar o Security Hub e garantir uma cobertura de segurança adequada para sua organização.

A configuração central permite que o administrador delegado personalize o Security Hub em várias contas e regiões da organização, em vez de configurar região por região. É possível criar uma política de configuração para toda a organização ou criar políticas de configuração diferentes para contas e OUs diferentes. As políticas especificam se o Security Hub está habilitado ou desabilitado nas contas associadas e quais padrões e controles de segurança estão habilitados.

O administrador delegado pode designar contas como sendo gerenciadas centralmente ou autogerenciadas. As contas gerenciadas centralmente só podem ser configuradas pelo administrador delegado. As contas autogerenciadas podem especificar suas próprias configurações.

Se você não fizer a adesão à configuração central, o administrador delegado terá uma capacidade mais limitada de configurar o Security Hub, chamada de configuração local. Sob a configuração local, o administrador delegado poderá habilitar automaticamente o Security Hub e os padrões de segurança padrão em novas contas da organização na região atual. Contudo, as contas existentes não usam essas configurações, de forma que podem ocorrer desvios na configuração após a entrada de uma conta na organização.

Além dessas novas configurações de conta, a configuração local é específica da conta e específica da região. Cada conta da organização deve configurar o serviço, os padrões e os controles do Security Hub separadamente em cada região. A configuração local também não oferece suporte ao uso de políticas de configuração.

Gerenciamento de contas manualmente por convite

Você deverá gerenciar manualmente as contas dos membros por convite no Security Hub se tiver uma conta independente ou se não estiver integrado ao Organizations. Uma conta independente não pode ser integrada ao Organizations, então é necessário gerenciá-la manualmente. Recomendamos a integração com o AWS Organizations e o uso da configuração central caso você adicione outras contas no futuro.

Ao usar o gerenciamento manual de contas, você designa uma conta para ser o administrador do Security Hub. A conta do administrador pode visualizar dados nas contas dos membros e realizar determinadas ações sobre as descobertas da conta do membro. O administrador do Security Hub convida outras contas para serem contas-membro, e o relacionamento administrador-membro é estabelecido quando uma conta-membro em potencial aceita o convite.

O gerenciamento manual de contas não oferece suporte ao uso de políticas de configuração. Sem políticas de configuração, o administrador não pode personalizar centralmente o Security Hub definindo configurações variáveis para contas diferentes. Em vez disso, cada conta da organização deve habilitar e configurar o Security Hub separadamente em cada região. Isso pode tornar mais difícil e demorado garantir uma cobertura de segurança adequada em todas as contas e regiões nas quais você usa o Security Hub. Isso também pode causar desvios na configuração, pois as contas dos membros podem especificar suas próprias configurações sem a intervenção do administrador.

Para gerenciar contas por convite, consulte Gerenciando contas por convite.

Gerenciando contas com AWS Organizations

Você pode integrar AWS Security Hub e gerenciar o Security Hub para contas em sua organização. AWS Organizations

Para integrar o Security Hub com AWS Organizations, você cria uma organização em AWS Organizations. A conta de gerenciamento do Organizations designa uma conta como administrador delegado do Security Hub para a organização. O administrador delegado pode então habilitar o Security Hub para outras contas na organização, adicionar essas contas como contas-membro do Security Hub e realizar as ações permitidas nas contas-membro. O administrador delegado do Security Hub pode habilitar e gerenciar o Security Hub com até 10.000 contas-membro.

A extensão das habilidades de configuração do administrador delegado depende de você usar a configuração central. Com a configuração central habilitada, você não precisa configurar o Security Hub separadamente em cada conta-membro e Região da AWS. O administrador delegado pode aplicar configurações específicas do Security Hub em contas-membro e unidades organizacionais (OUs) especificadas em todas as regiões.

A conta de administrador delegado do Security Hub pode realizar as ações a seguir em contas-membro:

- Se estiver usando a configuração central, configure centralmente o Security Hub para contas-membro e OUs criando políticas de configuração do Security Hub. As políticas de configuração podem ser usadas para habilitar e desabilitar o Security Hubhabilitar e desabilitar padrões e habilitar e desabilitar controles.
- Trate automaticamente as novas contas como contas-membro do Security Hub quando elas são adicionadas à organização. Se você usa a configuração central, uma política de configuração associada a uma OU inclui contas novas e existentes que fazem parte da OU.
- Tratar as contas existentes da organização como contas-membro do Security Hub. Isso acontecerá automaticamente se você usar a configuração central.
- Desassociar contas-membro que pertencem à organização. Se você usar a configuração central, poderá desassociar uma conta-membro somente depois de designá-la como autogerenciada. Como alternativa, é possível associar uma política de configuração que desabilite o Security Hub a contas específicas de membros gerenciadas centralmente.

Para obter uma lista completa das ações que o administrador delegado pode realizar nas contas dos membros, consulte Ações permitidas para contas.

Os tópicos desta seção explicam como integrar o Security Hub AWS Organizations e como gerenciar o Security Hub para contas em uma organização. Quando relevante, cada seção identifica os benefícios e as diferenças de gerenciamento para os usuários da configuração central.

Tópicos

Integrando o Security Hub com AWS Organizations

Para integrar AWS Security Hub e AWS Organizations, você cria uma organização no Organizations e usa a conta de gerenciamento da organização para designar uma conta delegada de administrador do Security Hub. O administrador delegado pode então habilitar o Security Hub para contas-membro, visualizar dados em contas-membro e realizar outras ações permitidas em contas-membro.

Se você usar a configuração central, o administrador delegado também poderá criar políticas de configuração do Security Hub que especifiquem como o serviço, os padrões e os controles do Security Hub devem ser configurados nas contas da organização.

Criar uma organização

Uma organização é uma entidade que você cria para consolidar a sua Contas da AWS , de forma que você possa administrá-la como uma única unidade.

Você pode criar uma organização usando o AWS Organizations console ou usando um comando das APIs do SDK AWS CLI ou de uma delas. Para obter instruções detalhadas, consulte Criação de uma organização no Guia do usuário doAWS Organizations .

Você pode usar AWS Organizations para visualizar e gerenciar centralmente todas as contas em sua organização. Uma organização tem uma conta de gerenciamento primária com zero ou mais contas-membro. É possível organizar as contas em uma estrutura de árvore hierárquica, com uma raiz na parte superior e unidades organizacionais (OUs) aninhadas sob a raiz. Cada conta pode estar diretamente sob raiz ou posicionada em uma das OUs na hierarquia. Uma OU é um contêiner para

contas específicas. Por exemplo, é possível criar uma OU de finanças que inclua todas as contas relacionadas a operações financeiras.

Recomendações para escolher o administrador delegado do Security Hub

Se você tiver uma conta de administrador criada a partir do processo de convite manual e estiver fazendo a transição para o gerenciamento de contas com AWS Organizations, o Security Hub recomenda que você designe essa conta como administrador delegado do Security Hub.

Você não deve designar a conta de gerenciamento da organização como administrador delegado do Security Hub. Isso ocorre porque os usuários que têm acesso à conta de gerenciamento da organização para gerenciar o faturamento provavelmente são diferentes dos usuários que precisam acessar o Security Hub para gerenciamento de segurança.

Recomendamos o uso da mesma conta de administrador delegado nas regiões. Se você optar pela configuração central, o Security Hub designará automaticamente o mesmo administrador delegado em sua região inicial e em qualquer região vinculada.

Verifique as permissões para configurar o administrador delegado do Security Hub

Para designar e remover uma conta delegada de administrador do Security Hub, a conta de gerenciamento da organização deve ter permissões para as `DisableOrganizationAdminAccount` ações `EnableOrganizationAdminAccount` e no Security Hub. A conta de gerenciamento do Organizations também deve ter permissões administrativas para o Organizations.

Para conceder todas as permissões necessárias, anexe as seguintes políticas gerenciadas do Security Hub ao diretor do IAM da conta de gerenciamento da organização:

- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess

Designando o administrador delegado do Security Hub

Para designar a conta delegada de administrador do Security Hub, você pode usar o console do Security Hub, a API do Security Hub ou. AWS CLIO Security Hub define o administrador delegado Região da AWS somente no atual, e você deve repetir a ação em outras regiões. Se você começar a usar a configuração central, o Security Hub definirá automaticamente o mesmo administrador delegado na região inicial e nas regiões vinculadas.

A conta de gerenciamento da organização não precisa habilitar o Security Hub para designar a conta delegada de administrador do Security Hub.

Recomendamos que a conta de gerenciamento da organização não seja a conta delegada do administrador do Security Hub. No entanto, se você escolher a conta de gerenciamento da organização como administrador delegado do Security Hub, a conta de gerenciamento deverá ter o Security Hub ativado. Se a conta de gerenciamento não tiver o Security Hub habilitado, você deverá habilitar o Security Hub para ela manualmente. O Security Hub não pode ser ativado automaticamente para a conta de gerenciamento da organização.

> **Note**
>
> Você deve designar o administrador delegado do Security Hub usando um dos métodos a seguir. A designação do administrador delegado do Security Hub com as APIs do Organizations não se reflete no Security Hub.
> Escolha seu método preferido e siga as etapas para designar a conta delegada do administrador do Security Hub.

Security Hub console

Para designar o administrador delegado do Security Hub durante a integração

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. Escolha Ir para o Security Hub. Você será solicitado a entrar na conta de gerenciamento da organização.
3. Na página Designar administrador delegado, na seção Conta de administrador delegado, especifique a conta de administrador delegado. Recomendamos escolher o mesmo administrador delegado que você definiu para outros serviços de segurança e conformidade da AWS .
4. Escolha Definir administrador delegado. Você deverá entrar na conta de administrador delegado (se ainda não tiver feito isso) para continuar a integração com a configuração central. Se não quiser iniciar a configuração central, escolha Cancelar. Seu administrador delegado está definido, mas você ainda não está usando a configuração central.

Para designar o administrador delegado do Security Hub na página Configurações

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

2. No painel de navegação do Security Hub, escolha Configurações. Em seguida, escolha Geral.
3. Se uma conta de administrador do Security Hub estiver atualmente atribuída, então antes de designar uma nova conta, você deverá remover a conta atual.

   Para remover a conta atual, em Administrador delegado, escolha Remover.
4. Insira o ID da conta que você deseja designar como conta de administrador do Security Hub.

   É necessário designar a mesma conta de administrador do Security Hub em todas as regiões. Se você designar uma conta diferente da conta designada em outras regiões, o console retornará um erro.
5. Escolha Delegar.

Security Hub API

Invoque a EnableOrganizationAdminAccountAPI a partir da conta de gerenciamento da organização. Forneça a Conta da AWS ID da conta delegada do administrador do Security Hub.

AWS CLI

Execute o enable-organization-admin-accountcomando na conta de gerenciamento da organização. Forneça a Conta da AWS ID da conta delegada do administrador do Security Hub.

Exemplo de comando:

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

Removendo o administrador delegado do Security Hub

> **Warning**
>
> Ao usar a configuração central, você não pode usar o console do Security Hub ou as APIs do Security Hub para alterar ou remover a conta do administrador delegado. Se a conta de gerenciamento da organização usar o AWS Organizations console ou as AWS Organizations APIs para alterar ou remover o administrador delegado do Security Hub, o Security Hub interromperá automaticamente a configuração central e excluirá suas políticas de configuração e associações de políticas. As contas-membro retêm as configurações que tinham antes de o administrador delegado ser alterado ou removido.

Somente a conta de gerenciamento da organização pode remover a conta delegada do administrador do Security Hub.

Para alterar o administrador delegado do Security Hub, você deve primeiro remover a conta atual do administrador delegado e depois designar uma nova.

Se você usar o console do Security Hub para remover o administrador delegado em uma região, ele será removido automaticamente em todas as regiões.

A API do Security Hub remove somente a conta delegada do administrador do Security Hub da região em que a chamada ou o comando da API é emitido. Você deve repetir a ação em outras regiões.

Se você usar a API Organizations para remover a conta delegada do administrador do Security Hub, ela será removida automaticamente em todas as regiões.

Removendo o administrador delegado do Security Hub (Organizations API, AWS CLI)

Você pode usar Organizations para remover o administrador delegado do Security Hub em todas as regiões.

Se você usar a configuração central para gerenciar contas, a remoção da conta de administrador delegado resultará na exclusão de suas políticas de configuração e associações de políticas. As contas-membro retêm as configurações que tinham antes de o administrador delegado ser alterado ou removido. Entretanto, essas contas não poderão mais ser gerenciadas pela conta de administrador delegado removida. Elas se tornam contas autogerenciadas que devem ser configuradas separadamente em cada região.

Escolha seu método preferido e siga as instruções para remover a conta delegada do administrador do Security Hub com AWS Organizations.

AWS Organizations API

Para remover o administrador delegado do Security Hub

Invoque a API DeregisterDelegatedAdministrator. Forneça o ID da conta do administrador delegado e a entidade principal do serviço para o Security Hub, que é `securityhub.amazonaws.com`.

AWS CLI

Para remover o administrador delegado do Security Hub

Execute o comando deregister-delegated-administrator. Forneça o ID da conta do administrador delegado e a entidade principal do serviço para o Security Hub, que é `securityhub.amazonaws.com`.

```
aws organizations deregister-delegated-administrator --account-id <admin account ID>
 --service-principal <Security Hub service principal>
```

Exemplo

```
aws organizations deregister-delegated-administrator --account-id 123456789012 --
service-principal securityhub.amazonaws.com
```

Removendo o administrador delegado do Security Hub (console do Security Hub)

Você pode usar o console do Security Hub para remover o administrador delegado do Security Hub em todas as regiões.

Quando a conta delegada do administrador do Security Hub é removida, as contas dos membros são desassociadas da conta de administrador delegada do Security Hub removida.

O Security Hub ainda está habilitado nas contas-membro. Elas se tornam contas independentes até que um novo administrador do Security Hub as habilite como contas-membro.

Se a conta de gerenciamento da organização não for uma conta habilitada no Security Hub, use a opção na página Bem-vindo ao Security Hub.

Para remover a conta de administrador delegada do Security Hub da página Bem-vindo ao Security Hub

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. Escolha Ir para o Security Hub.
3. Em Administrador delegado, escolha Remover.

Se a conta de gerenciamento da organização for uma conta habilitada no Security Hub, use a opção na guia Geral da página Configurações.

Para remover a conta de administrador delegada do Security Hub da página Configurações

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

2. No painel de navegação do Security Hub, escolha Configurações. Em seguida, escolha Geral.
3. Em Administrador delegado, escolha Remover.

Removendo o administrador delegado do Security Hub (API do Security Hub) AWS CLI

Você pode usar a API do Security Hub ou as operações do Security Hub AWS CLI para remover o administrador delegado do Security Hub. Quando você remove o administrador delegado com um desses métodos, ele só é removido na região onde o comando ou a chamada de API foram emitidos. O Security Hub não atualiza outras regiões e não remove a conta de administrador delegado em AWS Organizations.

Escolha seu método preferido e siga estas etapas para remover a conta delegada de administrador do Security Hub com o Security Hub.

Security Hub API

Para remover o administrador delegado do Security Hub

Usando as credenciais da conta de gerenciamento da organização, invoque a DisableOrganizationAdminAccountAPI. Forneça o ID da conta delegada do administrador do Security Hub.

AWS CLI

Para remover o administrador delegado do Security Hub

Usando as credenciais da conta de gerenciamento da organização, execute o disable-organization-admin-accountcomando. Forneça o ID da conta delegada do administrador do Security Hub.

```
aws securityhub disable-organization-admin-account --admin-account-id <admin account
 ID>
```

Exemplo

```
aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```

Habilitação automática do Security Hub em novas contas da organização

Quando novas contas ingressam na sua organização, elas são adicionadas à lista na página Contas do AWS Security Hub console. Para contas da organização, o Tipo é Por organização. Por padrão, novas contas não se tornam membros do Security Hub quando ingressam na organização. O status delas é Não é membro. A conta de administrador delegado pode adicionar automaticamente novas contas como membros e habilitar o Security Hub nessas contas quando elas ingressam na organização.

> **Note**
>
> Embora muitas Regiões da AWS estejam ativas por padrão para você Conta da AWS, você deve ativar determinadas regiões manualmente. Essas regiões são chamadas de regiões opcionais neste documento. Para habilitar automaticamente o Security Hub em uma nova conta em uma região opcional, a conta deve ter essa região ativada primeiro. Somente o proprietário da conta pode ativar a região de inscrição. Para obter mais informações sobre regiões opcionais, consulte Especificar quais Regiões da AWS sua conta pode usar.

Esse processo é diferente dependendo de você usar a configuração central (recomendada) ou a configuração local.

Habilitação automática de novas contas da organização (configuração central)

Se você usar a configuração central, poderá habilitar automaticamente o Security Hub em contas novas e existentes da organização criando uma política de configuração na qual o Security Hub esteja ativado. Em seguida, você pode associar a política à raiz da organização ou às unidades organizacionais (OUs) específicas.

Se você associar uma política de configuração na qual o Security Hub esteja habilitado a uma OU específica, o Security Hub será habilitado automaticamente em todas as contas (existentes e novas) que pertençam a essa OU. As novas contas que não pertençam à OU são autogerenciadas e não têm o Security Hub habilitado automaticamente. Se você associar uma política de configuração na qual o Security Hub esteja habilitado à raiz, o Security Hub será habilitado automaticamente em todas as contas (existentes e novas) que ingressem na organização. As exceções são se uma conta usar uma política diferente por meio de aplicação ou herança, ou se for autogerenciada.

Em sua política de configuração, você também pode definir quais padrões e controles de segurança devem ser habilitados na OU. Para gerar descobertas de controle para padrões habilitados, as

contas na OU devem estar AWS Config habilitadas e configuradas para registrar os recursos necessários. Para obter mais informações sobre AWS Config gravação, consulte Habilitando e configurando. AWS Config

Para obter instruções sobre como criar uma política de configuração, consulte Criação e associação de políticas de configuração do Security Hub.

Habilitação automática de novas contas da organização (configuração local)

Quando você usa a configuração local e ativa a habilitação automática, o Security Hub adiciona novas contas da organização como membros e habilita o Security Hub nelas na região atual. As outras regiões não são afetadas. Além disso, ativar a habilitação automática não habilita o Security Hub nas contas existentes da organização, a menos que elas já tenham sido adicionadas como contas-membro.

Depois de ativar a habilitação automática, os padrões de segurança padrão também serão habilitados automaticamente para novas contas na região atual quando elas ingressarem na organização. Os padrões padrão são AWS Foundational Security Best Practices (FSBP) e Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Não é possível alterar os padrões padrão. Se você quiser habilitar outros padrões em toda a organização ou habilitar padrões para contas e OUs selecionadas, recomendamos usar a configuração central.

Para gerar descobertas de controle para os padrões padrão (e outros padrões habilitados), as contas em sua organização devem estar AWS Config habilitadas e configuradas para registrar os recursos necessários. Para obter mais informações sobre AWS Config gravação, consulte Habilitando e configurando. AWS Config

Escolha seu método preferido e siga as etapas para habilitar automaticamente o Security Hub em novas contas da organização. Essas instruções se aplicam somente se você usar a configuração local.

Security Hub console

Para habilitar automaticamente novas contas da organização como membros do Security Hub

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

   Faça login usando as credenciais da conta do administrador delegado.
2. No painel de navegação do Security Hub, em Configurações, escolha Configuração.
3. Na seção Contas, ative a Habilitação automática de contas.

Security Hub API

Para habilitar automaticamente novas contas da organização como membros do Security Hub

Invoque a API `UpdateOrganizationConfiguration` a partir da conta do administrador delegado. Defina o campo `AutoEnable` como `true` para habilitar automaticamente o Security Hub nas novas contas da organização.

AWS CLI

Para habilitar automaticamente novas contas da organização como membros do Security Hub

Execute o comando `update-organization-configuration` a partir da conta do administrador delegado. Inclua o parâmetro `auto-enable` para habilitar automaticamente o Security Hub em novas contas da organização.

```
aws securityhub update-organization-configuration --auto-enable
```

Ativando manualmente o Security Hub em novas contas da organização

Se você não habilitar automaticamente o Security Hub em novas contas da organização quando elas entrarem na organização, você poderá adicionar essas contas como membros e habilitar o Security Hub nelas manualmente depois que elas entrarem na organização. Você também deve habilitar manualmente o Security Hub, Contas da AWS pois você se desassociou anteriormente de uma organização.

> **Note**
>
> Esta seção não se aplica a você se você usar a configuração central. Se você usar a configuração central, poderá criar políticas de configuração que habilitem o Security Hub em contas-membro e unidades organizacionais (OUs) especificadas. Você também pode habilitar padrões e controles específicos nessas contas e OUs.

Você não pode habilitar o Security Hub em uma conta se ela já for uma conta-membro em uma organização diferente.

Você também não pode habilitar o Security Hub em uma conta que esteja suspensa no momento. Se você tentar habilitar o serviço em uma conta suspensa, o status da conta mudará para Conta suspensa.

- Se a conta não tiver o Security Hub habilitado, o Security Hub será habilitado nessa conta. O padrão AWS Foundational Security Best Practices (FSBP) e o CIS AWS Foundations Benchmark v1.2.0 também estão habilitados na conta, a menos que você desative os padrões de segurança padrão.

  A exceção é a conta de gerenciamento do Organizations. O Security Hub não pode ser habilitado automaticamente na conta de gerenciamento do Organizations. Você deve habilitar manualmente o Security Hub na conta de gerenciamento do Organization antes de poder adicioná-lo como uma conta-membro.
- Se a conta já tiver o Security Hub habilitado, o Security Hub não fará nenhuma outra alteração na conta. Ele só habilita a participação como membro.

Para que o Security Hub gere descobertas de controle, as contas dos membros devem estar AWS Config habilitadas e configuradas para registrar os recursos necessários. Para obter mais informações, consulte Habilitar e configurar a AWS Config.

Escolha seu método preferido e siga as etapas para habilitar uma conta da organização como conta-membro do Security Hub.

Security Hub console

Para habilitar manualmente as contas da organização como membros do Security Hub

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

   Faça login usando as credenciais da conta do administrador delegado.
2. No painel de navegação do Security Hub, em Configurações, escolha Configuração.
3. Na lista Contas, selecione cada conta da organização que você deseja habilitar.
4. Escolha Ações e, em seguida, escolha Adicionar membro.

Security Hub API

Para habilitar manualmente as contas da organização como membros do Security Hub

Invoque a API `CreateMembers` a partir da conta do administrador delegado. Para que cada conta seja habilitada, forneça o ID da conta.

Ao contrário do processo de convite manual, quando você invocar `CreateMembers` para habilitar uma conta da organização, você não precisará enviar um convite.

AWS CLI

Para habilitar manualmente as contas da organização como membros do Security Hub

Execute o comando `create-members` a partir da conta do administrador delegado. Para que cada conta seja habilitada, forneça o ID da conta.

Ao contrário do processo de convite manual, quando você executar `create-members` para habilitar uma conta da organização, você não precisará enviar um convite.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

Exemplo

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

Desassociar contas-membro da sua organização

Para parar de receber e visualizar descobertas de uma conta de AWS Security Hub membro, você pode desassociar a conta de membro da sua organização.

> **Note**
>
> Se você usar a configuração central, a desassociação funcionará de forma diferente. É possível criar uma política de configuração que desabilite o Security Hub em uma ou mais contas-membro gerenciadas centralmente. Depois disso, essas contas ainda farão parte da organização, mas não gerarão descobertas do Security Hub. Se você usar a configuração central, mas também tiver contas-membro convidadas manualmente, será possível desassociar uma ou mais contas convidadas manualmente.

As contas de membros que são gerenciadas usando não AWS Organizations podem desassociar suas contas da conta de administrador. Somente a conta do administrador pode desassociar uma conta-membro.

A desassociação de uma conta-membro não fecha a conta. Em vez disso, ela remove a conta-membro da organização. A conta de membro desassociada se torna autônoma e não Conta da AWS é mais gerenciada pela integração do Security Hub com. AWS Organizations

Escolha seu método preferido e siga as etapas para desassociar uma conta-membro da organização.

Security Hub console

Para desassociar uma conta-membro de uma organização

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

   Faça login usando as credenciais da conta do administrador delegado.
2. No painel de navegação, em Configurações, selecione Configuração.
3. Na seção Contas, selecione as contas que você deseja desassociar. Se você usar a configuração central, poderá selecionar uma conta convidada manualmente para se dissociar na guia `Invitation accounts`. Essa guia ficará visível apenas se você usar a configuração central.
4. Escolha Ações e, em seguida, escolha Desassociar conta.

Security Hub API

Para desassociar uma conta-membro de uma organização

Invoque a API `DisassociateMembers` a partir da conta do administrador delegado. Você deve fornecer os Conta da AWS IDs para que as contas dos membros se desassociem. Para ver uma lista de contas-membro, invoque a API `ListMembers`.

AWS CLI

Para desassociar uma conta-membro de uma organização

Execute o comando `>disassociate-members` a partir da conta do administrador delegado. Você deve fornecer os Conta da AWS IDs para que as contas dos membros se desassociem. Para ver uma lista de contas-membro, execute o comando `>list-members`.

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

Exemplo

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Você também pode usar o AWS Organizations console ou os AWS CLI AWS SDKs para desassociar uma conta de membro da sua organização. Para obter mais informações, consulte Remoção de uma conta-membro da sua organização no Guia do usuário do AWS Organizations .

Desativando a integração do Security Hub com AWS Organizations

Depois que uma AWS Organizations organização é integrada AWS Security Hub, a conta de gerenciamento da Organizations pode posteriormente desativar a integração. Como um usuário da conta de gerenciamento do Organizations, é possível fazer isso desabilitando o acesso confiável para o Security Hub no AWS Organizations.

Quando você desabilita o acesso confiável para o Security Hub, ocorre o seguinte:

- O Security Hub perde seu status de serviço confiável em AWS Organizations.
- A conta de administrador delegado do Security Hub perde o acesso às configurações, dados e recursos do Security Hub para todas as contas-membro do Security Hub em todas as Regiões da AWS.
- Se você estava usando a configuração central, o Security Hub automaticamente deixará de usá-la em sua organização. Suas políticas de configuração e associações de políticas são excluídas. As contas retêm as configurações que tinham antes de você desabilitar o acesso confiável.
- Todas as contas-membro do Security Hub se tornam contas independentes e retêm suas configurações atuais. Se o Security Hub tiver sido habilitado para uma conta-membro em uma ou mais regiões, o Security Hub continuará habilitado para a conta nessas regiões. Os padrões e controles habilitados também permanecem inalterados. É possível alterar essas configurações separadamente em cada conta e região. Contudo, a conta não estará mais associada a um administrador delegado em nenhuma região.

Para obter informações adicionais sobre os resultados da desativação do acesso a serviços confiáveis, consulte Usando AWS Organizations com outros Serviços da AWS no Guia do AWS Organizations Usuário.

Para desativar o acesso confiável, você pode usar o AWS Organizations console, a API Organizations ou AWS CLI o. Somente um usuário da conta de gerenciamento do Organizations pode desabilitar o acesso confiável a serviços para o Security Hub. Para obter detalhes sobre as permissões necessárias, consulte Permissões necessárias para desativar o acesso confiável no Guia do AWS Organizations usuário.

Antes de desabilitar o acesso confiável, recomendamos trabalhar com o administrador delegado da sua organização para desabilitar o Security Hub em contas-membro e limpar os recursos do Security Hub nessas contas.

Escolha seu método preferido e siga as etapas para desabilitar o acesso confiável para o Security Hub.

Organizations console

Para desabilitar o acesso confiável para o Security Hub

1. Faça login no AWS Management Console usando as credenciais da conta de AWS Organizations gerenciamento.
2. Abra o console do Organizations em https://console.aws.amazon.com/organizations/.
3. No painel de navegação, escolha Serviços.
4. Em Serviços integrados, escolha AWS Security Hub.
5. Escolha Disable trusted access (Desabilitar acesso confiável).
6. Confirme que você deseja desativar o acesso confiável.

Organizations API

Para desabilitar o acesso confiável para o Security Hub

Invoque a AWSServiceAccess operação Disable da AWS Organizations API. No parâmetro `ServicePrincipal`, especifique a entidade principal de serviço do Security Hub (`securityhub.amazonaws.com`).

AWS CLI

Para desabilitar o acesso confiável para o Security Hub

Execute o disable-aws-service-accesscomando da AWS Organizations API. No parâmetro `service-principal`, especifique a entidade principal de serviço do Security Hub (`securityhub.amazonaws.com`).

Exemplo:

```
aws organizations disable-aws-service-access --service-principal
 securityhub.amazonaws.com
```

Gerenciando contas por convite

Você pode gerenciar centralmente várias AWS Security Hub contas de duas maneiras: integrando o Security Hub AWS Organizations ou enviando e aceitando manualmente os convites para membros. Você deve usar o processo manual se tiver uma conta independente ou se não estiver integrado ao Organizations. No gerenciamento manual de contas, o administrador do Security Hub convida as contas a se tornar membros. A relação administrador-membro é estabelecida quando uma conta-membro em potencial aceita o convite. Uma conta de administrador do Security Hub pode gerenciar o Security Hub para até 1.000 contas-membro baseadas em convites.

> **Tip**
>
> Se você criar uma organização baseada em convites no Security Hub, poderá, posteriormente, fazer a transição para usar o AWS Organizations em vez disso. Se você tiver mais de uma conta de membro, recomendamos gerenciar contas por meio de AWS Organizations.

A agregação entre regiões de descobertas e outros dados está disponível para contas que você convida por meio do processo de convite manual. No entanto, o administrador deve convidar a conta membro da região de agregação e de todas as regiões vinculadas para que a agregação entre regiões funcione. Além disso, a conta do membro deve ter o Security Hub ativado na região de agregação e em todas as regiões vinculadas para que o administrador possa visualizar as descobertas da conta do membro.

As políticas de configuração não são suportadas para contas de membros convidadas manualmente. Em vez disso, você deve definir as configurações do Security Hub separadamente em cada conta de membro e Região da AWS ao usar o processo de convite manual.

Você também deve usar o processo manual baseado em convites para contas que não pertençam à sua organização. Por exemplo, talvez não inclua uma conta de teste na sua organização. Ou talvez você queira consolidar contas de várias organizações em uma única conta de administrador do Security Hub. A conta de administrador do Security Hub deve enviar convites para contas pertencentes a outras organizações.

Na página Configuração do console do Security Hub, as contas que foram adicionadas por convite são listadas na guia Contas de convite. Se você usa a Como a configuração central funciona, mas também convida contas fora da sua organização, será possível ver as descobertas de contas

baseadas em convites nesta guia. Entretanto, o administrador do Security Hub não pode configurar contas baseadas em convites em todas as regiões por meio do uso de políticas de configuração.

Os tópicos desta seção explicam como gerenciar as contas membro por meio de convites.

Tópicos

Adicionar e convidar contas-membro

Sua conta se torna a AWS Security Hub administradora das contas que aceitam seu convite.

Quando você aceita um convite de outra conta, sua conta se torna uma conta-membro e essa conta se torna seu administrador.

Se sua conta for uma conta de administrador, você não poderá aceitar um convite para se tornar uma conta-membro.

Adicionar uma conta-membro consiste nas seguintes etapas:

1. A conta do administrador adiciona a conta do membro à lista de contas-membro.
2. A conta de administrador envia um convite para a conta-membro.
3. A conta-membro aceita o convite.

Adição de contas-membro

No console do Security Hub, é possível adicionar contas-membro para adicionar contas-membro. No console do Security Hub, é possível selecionar contas individualmente ou fazer upload de um arquivo `.csv` que contenha as informações das contas.

Para cada conta, você deve fornecer a ID da conta e um endereço de email. O endereço de email deve ser o endereço de email para contato sobre problemas de segurança na conta. Esse email não é usado para verificar a conta.

Escolha seu método preferido e siga as etapas para adicionar contas-membro.

Security Hub console

Para adicionar contas à sua lista de contas-membro

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

   Faça login no console do usando as credenciais de um administrador da .
2. No painel esquerdo, escolha Settings (Configurações).
3. Na página Configurações, selecione Contas e em seguida Adicionar contas. Em seguida, é possível adicionar contas individualmente ou fazer upload de um arquivo `.csv` que contenha a lista de contas.
4. Para selecionar as contas, siga um destes procedimentos:

   - Para adicionar as contas individualmente, em Inserir contas, insira o ID da conta e o endereço de email da conta a ser adicionada e selecione Adicionar.

     Repita este processo para cada conta.
   - Para usar um arquivo com valores separados por vírgula (.csv) para adicionar várias contas-membro, primeiro crie o arquivo. O arquivo deve conter o ID da conta e o endereço de email de cada conta a ser adicionada.

     Na sua lista `.csv`, as contas devem aparecer uma por linha. A primeira linha do arquivo `.csv` deve conter o cabeçalho. No cabeçalho, a primeira coluna é **`Account ID`** e a segunda coluna é **`Email`**.

     Cada linha subsequente precisa conter um ID de conta válido e um endereço de email da conta a ser adicionada.

     Aqui está um exemplo de um arquivo `.csv` quando visualizado em um editor de texto.

     ```
     Account ID,Email
     111111111111,user@example.com
     ```

     Em um programa de planilhas, os campos aparecem em colunas separadas. O formato subjacente ainda está separado por vírgula. Você deve formatar os IDs da conta como números não decimais. Por exemplo, a ID da conta 444455556666 não pode ser

formatada como 444455556666.0. Além disso, certifique-se de que a formatação numérica não remova nenhum zero à esquerda do ID da conta.

Para selecionar o arquivo, no console, selecione Lista de upload (.csv). Em seguida, selecione Procurar.

Depois de selecionar o arquivo, selecione Adicionar contas.

5. Depois de terminar de adicionar contas, em Contas a serem adicionadas, selecione Avançar.

Security Hub API

Para adicionar contas à sua lista de contas-membro

Invoque a API `CreateMembers` a partir da conta do administrador. Para que cada conta de membro seja adicionada, você deve fornecer o Conta da AWS ID.

AWS CLI

Para adicionar contas à sua lista de contas-membro

Execute o comando `create-members` a partir da conta do administrador. Para que cada conta de membro seja adicionada, você deve fornecer o Conta da AWS ID.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

Exemplo

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

Convite de contas-membro

Depois de adicionar contas-membro, você envia um convite para essas contas. Você também pode reenviar um convite para uma conta que já tenha desassociado do administrador.

Security Hub console

Para convidar contas-membro em potencial

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

Faça login no console do usando as credenciais de um administrador da .

2. No painel de navegação, selecione Configurações e em seguida Contas.
3. Para a conta a ser convidada, escolha Invite (Convidar) na coluna Status.
4. Quando solicitado, selecione Convidar para confirmar.

> **Note**
>
> Para reenviar convites a contas desassociadas, selecione cada conta desassociada na página Contas. Em Ações, selecione Reenviar convite.

Security Hub API

Para convidar contas-membro em potencial

Invoque a API `InviteMembers` a partir da conta do administrador. Para cada conta convidada, você deve fornecer o Conta da AWS ID.

AWS CLI

Para convidar contas-membro em potencial

Execute o comando `invite-members` a partir da conta do administrador. Para cada conta convidada, você deve fornecer o Conta da AWS ID.

```
aws securityhub invite-members --account-ids <accountIDs>
```

Exemplo

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

Responder a um convite para ser uma conta-membro

É possível aceitar ou recusar um convite para ser uma conta-membro.

Depois de aceitar um convite, sua conta se torna uma conta de AWS Security Hub membro. A conta que enviou o convite se torna sua conta de administrador do Security Hub. O usuário da conta de administrador pode visualizar as descobertas da sua conta-membro no Security Hub.

Se você recusar o convite, sua conta será marcada como Renunciada na lista de contas-membro da conta do administrador.

É possível aceitar apenas um convite para ser uma conta-membro.

Antes de poder aceitar ou recusar um convite, você deve habilitar o Security Hub.

Lembre-se de que todas as contas do Security Hub devem estar AWS Config habilitadas e configuradas para registrar todos os recursos. Para obter detalhes sobre a exigência de AWS Config, consulte Habilitando e configurando. AWS Config

Aceitar um convite

Escolha seu método preferido e siga as etapas para aceitar um convite para se tornar uma conta-membro.

Security Hub console

Para aceitar um convite para se tornar membro

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, selecione Configurações e em seguida Contas.
3. Na seção Conta do administrador, ative Aceitar e, em seguida, escolha Aceitar convite.

Security Hub API

Para aceitar um convite para se tornar membro

Invoque a API `AcceptAdministratorInvitation`. Você deve fornecer o identificador do convite e o Conta da AWS ID da conta do administrador. Para recuperar detalhes sobre o convite, use a operação `ListInvitations`.

AWS CLI

Para aceitar um convite para se tornar membro

Execute o comando `accept-administrator-invitation`. Você deve fornecer o identificador do convite e o Conta da AWS ID da conta do administrador. Para recuperar detalhes sobre o convite, execute o comando `list-invitations`.

```
aws securityhub accept-administrator-invitation --administrator-
id <administratorAccountID> --invitation-id <invitationID>
```

Exemplo

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --
invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

> **Note**
>
> O console do Security Hub continua usando `AcceptInvitation`. Eventualmente, ele mudará para usar `AcceptAdministratorInvitation`. Todas as políticas do IAM que controlam especificamente o acesso a essa função devem continuar usando `AcceptInvitation`. Você também deve adicionar `AcceptAdministratorInvitation` às suas políticas para garantir que as permissões corretas estejam em vigor após o início do uso do console `AcceptAdministratorInvitation`.

Recusar um convite

É possível recusar um convite para ser uma conta-membro. Quando você recusa um convite no console do Security Hub, sua conta é marcada como Renunciada na lista de contas-membro da conta do administrador.

Ao recusar um convite, você deve estar conectado à conta do membro que recebeu o convite.

Escolha seu método preferido e siga as etapas para recusar um convite para se tornar uma conta-membro.

Security Hub console

Para recusar um convite para se tornar membro

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, selecione Configurações e em seguida Contas.
3. Na seção Conta do administrador, selecione Recusar convite.

Security Hub API

Para recusar um convite para se tornar membro

Invoque a API `DeclineInvitations`. Você deve fornecer a Conta da AWS ID da conta do administrador que emitiu o convite. Para ver informações sobre seus convites, use a operação `ListInvitations`.

AWS CLI

Para recusar um convite para se tornar membro

Execute o comando `decline-invitations`. Você deve fornecer a Conta da AWS ID da conta do administrador que emitiu o convite. Para ver informações sobre seus convites, execute o comando `list-invitations`.

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

Exemplo

```
aws securityhub decline-invitations --account-ids "123456789012"
```

Desassociar contas-membro

Uma conta de AWS Security Hub administrador pode desassociar uma conta de membro para parar de receber e visualizar descobertas dessa conta. É necessário desassociar uma conta-membro antes de excluí-la.

Quando você desassocia uma conta-membro, ela permanece na sua lista de contas-membro com o status de Removida (Desassociada). Sua conta é removida das informações da conta do administrador da conta-membro.

Para continuar recebendo as descobertas da conta, é possível reenviar o convite. Para remover totalmente a conta-membro, é possível excluí-la.

Escolha seu método preferido e siga as etapas para desassociar uma conta-membro convidada manualmente da conta de administrador.

Security Hub console

Para desassociar uma conta-membro convidada manualmente

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

Faça login no console do usando as credenciais de um administrador da .

2. No painel de navegação, em Configurações, selecione Configuração.
3. Na seção Contas, selecione as contas que você deseja desassociar.
4. Escolha Ações e, em seguida, escolha Desassociar conta.

Security Hub API

Para desassociar uma conta-membro convidada manualmente

Invoque a API `DisassociateMembers` a partir da conta do administrador. Você deve fornecer os Conta da AWS IDs das contas dos membros que você deseja desassociar. Para ver uma lista de contas-membro, use a operação `ListMembers`.

AWS CLI

Para desassociar uma conta-membro convidada manualmente

Execute o comando `disassociate-members` a partir da conta do administrador. Você deve fornecer os Conta da AWS IDs das contas dos membros que você deseja desassociar. Para ver uma lista de contas-membro, execute o comando `list-members`.

```
aws securityhub disassociate-members --account-ids <accountIds>
```

Exemplo

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Excluir contas-membro

Como conta de AWS Security Hub administrador, você pode excluir contas de membros que foram adicionadas por convite. Antes de poder excluir uma conta ativada, você deve desassociá-la.

Quando você exclui uma conta-membro, ela é completamente removida da lista. Para restaurar a associação da conta-membro, você deverá adicioná-la e convidá-la novamente, como se fosse uma conta-membro completamente nova.

Você não pode excluir contas que pertencem a uma organização e que são gerenciadas usando a integração com AWS Organizations.

Escolha seu método preferido e siga as etapas para excluir contas-membro manualmente convidadas.

Security Hub console

Para excluir uma conta-membro manualmente convidada

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

   Faça login com sua conta de administrador.
2. No painel de navegação, escolha Configurações e, em seguida, Configuração.
3. Escolha a guia Contas de convite. Em seguida, selecione as contas a serem excluídas.
4. Escolha Ações e, em seguida, escolha Excluir. Essa opção só estará disponível se você tiver desassociado a conta. É necessário desassociar uma conta-membro antes que ela possa ser excluída.

Security Hub API

Para excluir uma conta-membro manualmente convidada

Invoque a API `DeleteMembers` a partir da conta do administrador. Você deve fornecer os IDs das Conta da AWS das contas-membro que deseja excluir. Para recuperar a lista de contas-membro, invoque a API `ListMembers`.

AWS CLI

Para excluir uma conta-membro manualmente convidada

Execute o comando `delete-members` a partir da conta do administrador. Você deve fornecer os IDs das Conta da AWS das contas-membro que deseja excluir. Para recuperar a lista de contas-membro, execute o comando `list-members`.

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

Exemplo

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

Desassociando-se da sua conta de administrador

Se sua conta foi adicionada como conta de AWS Security Hub membro por convite, você pode desassociar a conta de membro da conta de administrador. Depois de desassociar uma conta-membro, o Security Hub não envia as descobertas da conta para a conta do administrador.

As contas de membros que são gerenciadas usando a integração com não AWS Organizations podem dissociar suas contas da conta de administrador. Somente o administrador delegado do Security Hub pode desassociar contas-membro que sejam gerenciadas com o Organizations.

Quando você se desassocia da sua conta de administrador, sua conta permanece na lista de membros da conta de administrador com o status de Renunciado. Entretanto, a conta do administrador não recebe nenhuma descoberta para sua conta.

Depois de você se dissociar da conta de administrador, o convite para ser membro ainda permanecerá. É possível aceitar o convite novamente no futuro.

Security Hub console

Para se dissociar da sua conta de administrador

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, selecione Configurações e em seguida Contas.
3. Na seção Conta do administrador, desative Aceitar e, em seguida, escolha Atualizar.

Security Hub API

Para se dissociar da sua conta de administrador

Invoque a API `DisassociateFromAdministratorAccount`.

AWS CLI

Para se dissociar da sua conta de administrador

Execute o comando `disassociate-from-administrator-account`.

```
aws securityhub disassociate-from-administrator-account
```

> **Note**
>
> O console do Security Hub continua usando `DisassociateFromMasterAccount`. Eventualmente, ele mudará para usar `DisassociateFromAdministratorAccount`. Todas as políticas do IAM que controlam especificamente o acesso a essa função devem continuar usando `DisassociateFromMasterAccount`. Você também deve adicionar `DisassociateFromAdministratorAccount` às suas políticas para garantir que as permissões corretas estejam em vigor após o início do uso do console `DisassociateFromAdministratorAccount`.

Transição para o AWS Organizations para gerenciamento de contas

Ao gerenciar contas manualmente no AWS Security Hub, você deverá convidar contas-membro em potencial e configurar cada conta-membro separadamente em cada Região da AWS.

Ao integrar o Security Hub e AWS Organizations, é possível eliminar a necessidade de enviar convites e obter mais controle sobre como o Security Hub é configurado e personalizado em sua organização.

É possível usar uma abordagem combinada na qual você usa a integração com o AWS Organizations, mas também convida manualmente contas de fora da sua organização. Entretanto, recomendamos usar exclusivamente a integração do Organizations. A configuração central, um recurso que ajuda você a gerenciar o Security Hub em várias contas e regiões, só está disponível quando você se integra ao Organizations.

Esta seção aborda como é possível fazer a transição do gerenciamento manual de contas baseado em convites para o gerenciamento de contas com o AWS Organizations.

Integração do Security Hub com o AWS Organizations

Primeiro, você deve integrar o Security Hub e o AWS Organizations.

É possível integrar esses serviços concluindo as etapas a seguir:

- Crie uma organização no AWS Organizations. Para obter instruções, consulte Criação de uma organização no Guia do usuário do AWS Organizations.
- A partir da conta de gerenciamento do Organizations, , designe uma conta de administrador delegado do Security Hub.

> **Note**
>
> A conta de gerenciamento da organização não pode ser definida como conta de DA.

Para obter instruções detalhadas, consulte Integrando o Security Hub com AWS Organizations.

Ao concluir as etapas anteriores, você concederá acesso confiável ao Security Hub no AWS Organizations. Isso também habilitará o Security Hub na Região da AWS atual para a conta do administrador delegado.

O administrador delegado pode gerenciar a organização no Security Hub, principalmente adicionando as contas da organização como contas-membro do Security Hub. O administrador também pode acessar determinadas configurações, dados e recursos do Security Hub para essas contas.

Quando você faz a transição para o gerenciamento de contas usando o Organizations, as contas baseadas em convites não se tornam automaticamente membros do Security Hub. Somente as contas que você adicionar à sua nova organização podem se tornar membros do Security Hub.

Configuração central versus configuração local

Depois de ativar a integração, será possível gerenciar contas com o Organizations. Para obter mais informações, consulte Gerenciando contas com AWS Organizations. O gerenciamento de contas varia de acordo com o tipo de configuração da sua organização.

Há dois tipos de configuração possíveis para sua organização, o local e o central. Seu tipo de configuração padrão é a configuração local. Para ver seu tipo de configuração atual, escolha Configurações no painel de navegação do console do Security Hub e, em seguida, Configuração. Você também pode invocar a API `DescribeOrganizationConfiguration` para ver seu tipo de configuração.

Na configuração local, a conta do administrador delegado pode optar por habilitar automaticamente o Security Hub e os padrões de segurança padrão em novas contas à medida que elas ingressam na organização. Essas novas configurações de conta entram em vigor na região atual. Outras configurações do Security Hub devem ser definidas separadamente por cada conta-membro em cada região.

Recomendamos usar a configuração central em vez da configuração local. Na configuração central, a conta do administrador delegado pode criar políticas de configuração do Security Hub que entrem

em vigor em várias regiões e especificar os recursos do Security Hub nas várias contas e unidades organizacionais (OUs) da sua organização. É possível aplicar uma única política de configuração em toda a sua organização ou políticas de configuração diferentes para contas e OUs diferentes. Por exemplo, é possível habilitar um conjunto de padrões e controles nas contas de produção e um conjunto diferente de padrões e controles nas contas de teste. O DA pode editar as políticas de configuração conforme necessário.

Para obter mais informações sobre como a configuração central funciona, consulte Como a configuração central funciona.

Para obter instruções sobre como alternar da configuração local para a central, consulte Comece a usar a configuração central.

Ações permitidas para contas

As contas de administrador e contas-membro têm acesso às ações do AWS Security Hub indicadas nas tabelas a seguir. Nas tabelas, os valores têm os significados a seguir:

- Qualquer: a conta pode realizar a ação para qualquer conta sob o mesmo administrador ou conta.
- Atual: a conta pode realizar a ação somente por si mesma (a conta na qual você está conectado no momento).
- Traço: indica que a conta não pode realizar a ação.

Conforme observado nas tabelas, as ações permitidas diferem com base em se você fez a integração com o AWS Organizations e no tipo de configuração que sua organização usa. Para obter informações sobre a diferença entre a configuração central e local, consulte Gerenciando contas com o AWS Organizations.

O Security Hub não copia as descobertas da conta-membro para a conta do administrador. No Security Hub, todas as descobertas são inseridas em uma região específica para uma conta específica. Em cada região, a conta do administrador pode visualizar e gerenciar as descobertas de suas contas de membros nessa região.

Se você definir uma região de agregação, a conta do administrador poderá visualizar e gerenciar as descobertas da conta-membro de regiões vinculadas que sejam replicadas para a região de agregação. Para obter mais informações sobre agregação entre regiões, consulte Agregação entre regiões.

Essa tabela reflete as permissões padrão para contas de administrador e membro. É possível usar políticas do IAM personalizadas para restringir ainda mais o acesso aos atributos e funções do Security Hub. Para obter orientação e exemplos, consulte a postagem do blog Alinhando as políticas do IAM às personas dos usuários para AWS Security Hub.

Ações permitidas se você se integrar ao Organizations e usar a configuração central

As contas de administrador e de membro podem acessar as ações do Security Hub da forma a seguir se você se integrar ao Organizations e usar a configuração central.

Ação	Conta de administrador delegado do Security Hub	Conta-membro gerenciada centralmente	Conta-membro autogerenciada
Crie e gerencie políticas de configuração do Security Hub	Para contas gerenciadas automaticamente e centralmente	–	–
Visualizar contas da organização	Any	–	–
Desassociar conta-membro	Any	–	–
Excluir conta-membro	Qualquer conta que não seja da organização	–	–
Desabilitar o Security Hub	Para a conta atual e contas gerenciadas centralmente	–	Atual
Veja as descobertas e o histórico de descobertas	Any	Atual	Atual
Atualizar as descobertas	Any	Atual	Atual

Ação	Conta de administrador delegado do Security Hub	Conta-membro gerenciada centralmente	Conta-membro autogerenciada
Visualizar resultados do insight	Any	Atual	Atual
Visualizar detalhes do controle	Any	Atual	Atual
Ative ou desative as descobertas de controle consolidadas	Any	–	–
Habilitar e desabilitar padrões	Para a conta atual e contas gerenciadas centralmente	–	Atual
Habilitar e desabilitar controles	Para a conta atual e contas gerenciadas centralmente	–	Atual
Habilitar e desabilitar integrações	Atual	Atual	Atual
Configurar uma agregação entre regiões	Any	–	–
Selecione a região inicial e as regiões vinculadas	Qualquer (é necessário parar e reiniciar a configuração central para alterar a região inicial)	–	–
Configurar ações personalizadas	Atual	Atual	Atual

Ação	Conta de administrador delegado do Security Hub	Conta-membro gerenciada centralmente	Conta-membro autogerenciada
Configurar regras de automação	Any	–	–
Configurar insights personalizados	Atual	Atual	Atual

Ações permitidas se você se integrar ao Organizations e usar a configuração local

As contas de administrador e de membro podem acessar as ações do Security Hub da forma a seguir se você se integrar ao Organizations e usar a configuração local.

Ação	Conta de administrador delegado do Security Hub	Conta-membro
Crie e gerencie políticas de configuração do Security Hub	–	–
Visualizar contas da organização	Any	–
Desassociar conta-membro	Any	–
Excluir conta-membro	–	–
Desabilitar o Security Hub	–	Atual (se a conta for desassociada do administrador delegado)
Veja as descobertas e o histórico de descobertas	Any	Atual
Atualizar as descobertas	Any	Atual

Ação	Conta de administrador delegado do Security Hub	Conta-membro
Visualizar resultados do insight	Any	Atual
Visualizar detalhes do controle	Any	Atual
Ative ou desative as descobertas de controle consolidadas	Any	–
Habilitar e desabilitar padrões	Atual	Atual
Habilita automaticamente o Security Hub e os padrões padrão em novas contas da organização	Para a conta atual e novas contas da organização	–
Habilitar e desabilitar controles	Atual	Atual
Habilitar e desabilitar integrações	Atual	Atual
Configurar uma agregação entre regiões	Any	–
Configurar ações personalizadas	Atual	Atual
Configurar regras de automação	Any	–
Configurar insights personalizados	Atual	Atual

Ações permitidas para contas baseadas em convites

As contas de administrador e de membro podem acessar as ações do Security Hub da forma a seguir se você usar o método baseado em convite para gerenciar contas manualmente em vez de integrá-las com o AWS Organizations.

Ação	Conta de administrador do Security Hub	Conta-membro
Crie e gerencie políticas de configuração do Security Hub	–	–
Visualizar contas da organização	Any	–
Desassociar conta-membro	Any	Atual
Excluir conta-membro	Any	–
Desabilitar o Security Hub	Atual (se não houver contas-membro habilitadas)	Atual (se a conta for desassociada da conta do administrador)
Veja as descobertas e o histórico de descobertas	Any	Atual
Atualizar as descobertas	Any	Atual
Visualizar resultados do insight	Any	Atual
Visualizar detalhes do controle	Any	Atual
Ative ou desative as descobertas de controle consolidadas	Any	–
Habilitar e desabilitar padrões	Atual	Atual
Habilita automaticamente o Security Hub e os padrões	–	–

Ação	Conta de administrador do Security Hub	Conta-membro
padrão em novas contas da organização		
Habilitar e desabilitar controles	Atual	Atual
Habilitar e desabilitar integrações	Atual	Atual
Configurar uma agregação entre regiões	Any	–
Configurar ações personali zadas	Atual	Atual
Configurar regras de automação	Any	–
Configurar insights personali zados	Atual	Atual

Restrições e recomendações sobre o gerenciamento de contas

A seção a seguir resume algumas restrições e recomendações que você deve ter em mente ao gerenciar contas-membro no AWS Security Hub.

Número máximo de contas-membro

Se você usar a integração com AWS Organizations, o Security Hub suporta até 10.000 contas de membros por conta de administrador delegado em cada uma Região da AWS. Se você habilitar e gerenciar o Security Hub manualmente, o Security Hub suportará até 1.000 convites de conta de membro por conta de administrador em cada região.

Contas e regiões

Associação por organização

Se você integrar o Security Hub com AWS Organizations, a conta de gerenciamento do Organizations pode designar uma conta de administrador delegado (DA) para o Security Hub. A conta de gerenciamento da organização não pode ser definida como o DA no Organizations. Embora isso seja permitido no Security Hub, recomendamos que a conta de gerenciamento do Organizations não seja a do DA.

Recomendamos que você escolha a mesma conta de DA em todas as regiões. Se você usar a configuração central, o Security Hub definirá a mesma conta de DA em todas as regiões nas quais você configurar o Security Hub para sua organização.

Também recomendamos que você escolha a mesma conta DA em todos os serviços de AWS segurança e conformidade para ajudá-lo a gerenciar problemas relacionados à segurança em um único painel.

Associação por convite

Para contas-membro criadas por convite, a associação entre as contas de administrador e membro é criada somente na região de onde o convite é enviado. A conta de administrador deve habilitar o Security Hub em cada região em que você deseja usá-la. A conta de administrador convidará então cada conta a se ternar uma conta-membro nessa região.

Restrições nas relações administrador-membro

> **Note**
>
> Se você usa a integração do Security Hub com AWS Organizations, e não convidou manualmente nenhuma conta de membro, esta seção não se aplica a você.

Uma conta não pode ser uma conta de administrador e uma conta-membro ao mesmo tempo.

Uma conta-membro só pode ser associada a uma conta de administrador. Se uma conta da organização for habilitada pela conta de administrador do Security Hub, a conta não poderá aceitar um convite de outra conta. Se uma conta já tiver aceitado um convite, ela não poderá ser habilitada

pela conta de administrador do Security Hub para a organização. Ela também não pode receber convites de outras contas.

Para o processo de convite manual, aceitar um convite de associação é opcional.

Coordenar contas de administrador entre serviços

O Security Hub agrega descobertas de vários AWS serviços, como Amazon GuardDuty, Amazon Inspector e Amazon Macie. O Security Hub também permite que os usuários partam de uma GuardDuty descoberta para iniciar uma investigação no Amazon Detective.

Entretanto, as relações administrador-membro configuradas nesses outros serviços não se aplicam automaticamente ao Security Hub. O Security Hub recomenda que você use a mesma conta da conta de administrador para todos esses serviços. Essa conta de administrador deve ser uma conta responsável pelas ferramentas de segurança. A mesma conta também deve ser a conta agregadora do AWS Config.

Por exemplo, um usuário da conta de GuardDuty administrador A pode ver as descobertas das contas de GuardDuty membros B e C no GuardDuty console. Se a conta A ativar o Security Hub, os usuários da conta A não verão automaticamente GuardDuty as descobertas das contas B e C no Security Hub. Uma relação administrador-membro do Security Hub também é necessária para essas contas.

Para fazer isso, torne a conta A a conta de administrador do Security Hub e habilite as contas B e C para se tornarem contas-membro do Security Hub.

Efeito das ações da conta nos dados do Security Hub

Essas ações da conta têm os seguintes efeitos nos dados do AWS Security Hub.

Security Hub desabilitado

Se você usar a configuração central, o administrador delegado (DA) poderá criar políticas de configuração do Security Hub que desabilitem o AWS Security Hub em contas e unidades organizacionais (OUs) específicas. Nesse caso, o Security Hub será desabilitado nas contas e OUs especificadas em sua região inicial e em qualquer região vinculada.

Se você não usa a configuração central, deverá desabilitar o Security Hub separadamente em cada conta e região onde ele tenha sido habilitado.

Nenhuma descoberta nova será gerada para a conta de administrador se o Security Hub estiver desabilitado na conta do administrador. Você também não pode usar a configuração central se o Security Hub estiver desabilitado na conta do DA. As descobertas existentes serão excluídas após 90 dias.

As integrações com outros Serviços da AWS são removidas.

Os padrões e controles de segurança habilitados são desabilitados.

Outros dados e configurações do Security Hub, inclusive ações personalizadas, insights e assinaturas de produtos de terceiros são retidas.

Conta-membro desassociada da conta de administrador

Quando uma conta-membro é desassociada da conta de administrador, esta perde a permissão para visualizar as descobertas na conta do membro. Contudo, o Security Hub ainda estará habilitado em ambas as contas.

Se você usar a configuração central, o DA não poderá configurar o Security Hub para uma conta-membro que esteja desassociada da conta do DA.

Configurações personalizadas ou integrações definidas para a conta de administrador não são aplicadas às descobertas da conta-membro antiga. Por exemplo, depois que as contas forem desassociadas, será possível ter uma ação personalizada na conta de administrador usada como padrão de evento em uma regra do Amazon EventBridge. Entretanto, essa ação personalizada não pode ser usada na conta-membro.

Na lista Contas da conta de administrador do Security Hub, uma conta removida tem o status de Desassociada.

A conta-membro é removida de uma organização

Quando uma conta-membro é removida de uma organização, a conta de administrador do Security Hub perde a permissão para visualizar as descobertas na conta-membro. Entretanto, o Security Hub ainda estará habilitado em ambas as contas com as mesmas configurações que tinham antes da remoção.

Se você usar a configuração central, não poderá configurar o Security Hub para uma conta-membro depois que ela for removida da organização à qual o administrador delegado pertence.

Entretanto, a conta reterá as configurações que tinha antes da remoção, a menos que você as altere manualmente.

Na lista Contas da conta de administrador do Security Hub, uma conta removida tem o status de Excluída.

A conta é suspensa

Quando uma conta é suspensa na AWS, ela perde a permissão para ver suas descobertas no Security Hub. Nenhuma nova descoberta é gerada para essa conta. A conta de administrador de uma conta suspensa pode ver as descobertas da conta existente.

Para uma conta da organização, o status da conta-membro também pode mudar para Conta suspensa. Isso acontece se a conta for suspensa ao mesmo tempo em que a conta de administrador tenta habilitá-la. A conta de administrador de uma conta suspensa pode ver as descobertas da conta existente. Do contrário, o status de suspensa não afetará o status da conta-membro.

Se você usar a configuração central, a associação de políticas falhará se o administrador delegado tentar associar uma política de configuração a uma conta suspensa.

Após 90 dias, a conta é encerrada ou reativada. Quando a conta é reativada, suas permissões do Security Hub são restauradas. Se o status da conta-membro for Conta suspensa, a conta de administrador deverá habilitar a conta manualmente.

A conta é fechada

Quando uma Conta da AWS é fechada, o Security Hub responde ao fechamento da seguinte forma.

O Security Hub manterá as descobertas da conta por 90 dias a partir da data efetiva do fechamento da conta. Ao final do período de 90 dias, o Security Hub exclui permanentemente todos as descobertas da conta.

- Para reter descobertas por mais de 90 dias, é possível usar uma ação personalizada com uma regra do EventBridge para armazenar as descobertas no bucket do Amazon S3. Desde que o Security Hub retenha as descobertas, quando você reabre a conta fechada, o Security Hub restaura as descobertas da conta.
- Se a conta for uma conta de administrador do Security Hub, ela será removida como administrador e todas as contas de membro serão removidas. Se a conta for uma conta-membro, ela será desassociada e removida como membro da conta de administrador do Security Hub.

- Para obter mais informações, consulte Fechamento de uma conta no Guia do usuário de faturamento e gerenciamento de custos da AWS.

> **Important**
>
> Para clientes nas regiões do AWS GovCloud (US):
>
> - Antes de fechar sua conta, faça backup e, em seguida, exclua os dados da política e outros recursos da conta. Você não terá mais acesso a eles depois de fechar a conta.

Agregação entre regiões

Com a agregação entre regiões, é possível agregar descobertas, encontrar atualizações, insights, controlar os status de conformidade e pontuações de segurança de várias regiões em uma única região de agregação. Em seguida, é possível gerenciar todos esses dados da região de agregação.

> **Note**
>
> Em AWS GovCloud (US), a agregação entre regiões é suportada somente para descobertas, atualizações e insights transversais. AWS GovCloud (US) Especificamente, você só pode agregar descobertas, atualizações e insights entre AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA). Nas regiões da China, a agregação entre regiões é compatível somente com descobertas, atualizações de descobertas e insights das regiões da China. Especificamente, você só pode agregar descobertas, atualizações de descobertas e insights entre a China (Pequim) e a China (Ningxia).

Suponha que você defina Leste dos EUA (Norte da Virgínia) como região de agregação e Oeste dos EUA (Oregon) e Oeste dos EUA (N. da Califórnia) como regiões vinculadas. Ao visualizar a página de Descobertas no Leste dos EUA (Norte da Virgínia), você vê as descobertas de todas as três regiões. As atualizações dessas descobertas também se refletem nas três regiões.

O status de habilitação de um controle deve ser modificado em cada região. Se um controle estiver habilitado em uma região vinculada, mas desabilitado na região de agregação, será possível ver o status de conformidade do controle na região de agregação, mas esse controle não poderá ser habilitado ou desabilitado na região de agregação.

Para ver as pontuações de segurança e os status de conformidade entre regiões, adicione as seguintes permissões ao seu perfil do IAM que usa o Security Hub:

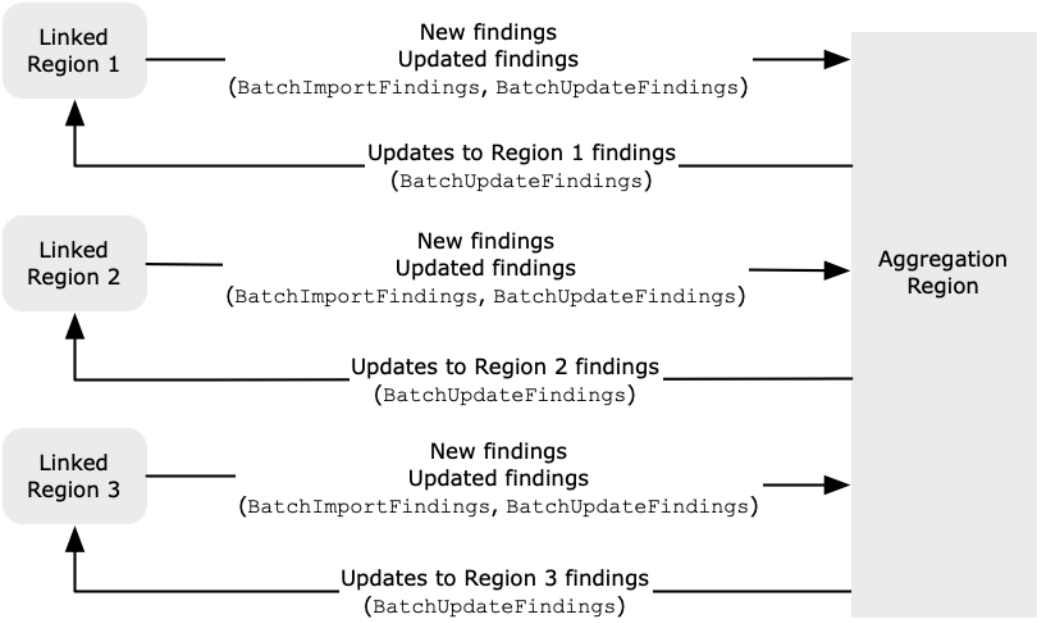
- `ListSecurityControlDefinitions`
- `BatchGetStandardsControlAssociations`
- `BatchUpdateStandardsControlAssociations`

Como funciona a agregação entre regiões

Quando a agregação entre regiões está habilitada, o Security Hub replica os seguintes dados das regiões vinculadas para a região de agregação. Isso ocorre em todas as contas que têm a agregação entre regiões ativada.

- Descobertas
- Insights
- Status de conformidade de controle
- Pontuações de segurança

Além dos novos dados na lista anterior, o Security Hub também replica as atualizações desses dados entre as regiões vinculadas e a região de agregação. As atualizações que ocorrem em uma região vinculada são replicadas na região de agregação. As atualizações que ocorrem na região de agregação são replicadas de volta para a região vinculada.



Se houver atualizações conflitantes na região de agregação e na região vinculada, a atualização mais recente será usada.

A agregação entre regiões não aumenta o custo do Security Hub. Você não é cobrado quando o Security Hub replica novos dados ou atualizações.

Na região de agregação, a página de Resumo fornece uma visão de suas descobertas ativas nas regiões vinculadas. Para obter informações, consulte Visualização de um resumo de descobertas entre regiões por gravidade. Outros painéis da página de Resumo que analisam as descobertas também exibem informações de todas as regiões vinculadas.

Suas pontuações de segurança na região de agregação são calculadas comparando o número de controles aprovados com o número de controles habilitados em todas as regiões vinculadas. Além disso, se um controle estiver habilitado em pelo menos uma região vinculada, ele estará visível nas páginas de detalhes dos Padrões de segurança da região de agregação. O status de conformidade dos controles nas páginas de detalhes dos padrões reflete as descobertas nas regiões vinculadas. Se uma verificação de segurança associada a um controle falhar em uma ou mais regiões vinculadas, o status de conformidade desse controle será exibido como Falha nas páginas de detalhes dos padrões da região de agregação. O número de verificações de segurança inclui descobertas de todas as regiões vinculadas.

O Security Hub agrega apenas dados de regiões em que uma conta tem o Security Hub habilitado. O Security Hub não é habilitado automaticamente para uma conta com base na configuração de agregação entre regiões.

Agregação para contas de administradores e membros

Contas autônomas, contas de membros e contas de administrador podem configurar a agregação entre regiões. Se configurada por um administrador, a presença da conta de administrador é essencial para que a agregação entre regiões funcione em contas administradas. Se a conta do administrador for removida ou desassociada de uma conta de membro, a agregação entre regiões da conta de membro será interrompida. Isso é verdade mesmo que a conta tenha ativado a agregação entre regiões antes do início do relacionamento administrador-membro.

Quando uma conta de administrador habilita a agregação entre regiões, o Security Hub replica os dados que a conta do administrador gera em todas as regiões vinculadas à região de agregação. Além disso, o Security Hub identifica as contas de membros associadas a esse administrador, e cada conta de membro herda as configurações de agregação entre regiões do administrador. O Security Hub replica os dados que uma conta membro gera em todas as regiões vinculadas à região de agregação.

O administrador pode acessar e gerenciar as descobertas de segurança de todas as contas dos membros nas regiões administradas. No entanto, como administrador do Security Hub, você deve estar conectado à região de agregação para visualizar dados agregados de todas as contas de membros e regiões vinculadas.

Como conta de membro do Security Hub, você deve estar conectado à região de agregação para ver os dados agregados da sua conta de todas as regiões vinculadas. As contas de membros não têm permissão para visualizar dados de outras contas de membros.

Uma conta de administrador pode convidar manualmente contas de membros ou servir como administrador delegado de uma organização integrada à AWS Organizations. Para uma conta de membro convidada manualmente, o administrador deve convidar a conta da região de agregação e de todas as regiões vinculadas para que a agregação entre regiões funcione. Além disso, a conta do membro deve ter o Security Hub ativado na região de agregação e em todas as regiões vinculadas para que o administrador possa visualizar as descobertas da conta do membro. Se você não usar a região de agregação para outros fins, poderá desativar os padrões e integrações do Security Hub nessa região para evitar cobranças.

Se você planeja usar a agregação entre regiões e tem várias contas de administrador, recomendamos seguir estas melhores práticas:

- Cada conta de administrador tem contas-membro diferentes.
- Cada conta de administrador tem as mesmas contas-membro em todas as regiões.
- Cada conta de administrador usa uma região de agregação diferente.

> **Note**
>
> Para entender como a agregação entre regiões afeta a configuração central, consulte. Configuração central e agregação entre regiões

Configuração central e agregação entre regiões

A configuração central é um recurso opcional no Security Hub que você pode usar se fizer a integração com o. AWS Organizations Se você usar a configuração central, a conta de administrador delegada poderá configurar o serviço, os padrões e os controles do Security Hub para contas e unidades organizacionais (OU) na organização. Para configurar contas e OUs, o administrador delegado cria políticas de configuração do Security Hub. As políticas de configuração podem ser usadas para definir se o Security Hub está habilitado ou desabilitado, e quais padrões e controles estão habilitados. O administrador delegado associa políticas de configuração a contas específicas, a OUs ou à raiz (toda a organização).

O administrador delegado pode criar e gerenciar políticas de configuração para a organização somente a partir da região de agregação. Além disso, as políticas de configuração entram em vigor na região de agregação e em todas as regiões vinculadas. Você não pode criar uma política de configuração que se aplique somente a algumas regiões vinculadas e não a outras. Na configuração central, a região de agregação é chamada de região inicial. A mesma região deve servir como região inicial para fins de configuração central e como região de agregação para fins de agregação entre regiões. Para obter informações sobre agregação entre regiões, consulte Agregação entre regiões.

Para usar a configuração central, você deve designar uma região de origem e pelo menos uma região vinculada.

Alterar suas configurações de agregação entre regiões pode afetar suas políticas de configuração. Quando você adiciona uma região vinculada, suas políticas de configuração entram em vigor nessa região. Se a região for uma região de adesão, ela deverá estar habilitada para que suas políticas de configuração entrem em vigor nela. Por outro lado, quando você remove uma região vinculada, as políticas de configuração não têm mais efeito nessa região. Nessa região, as contas mantêm as configurações que tinham quando a região vinculada foi removida. É possível alterar essas configurações, mas isso deve ser feito separadamente em cada conta e região.

Se você remover ou alterar a região inicial, suas políticas de configuração e associações de políticas serão excluídas. Não será mais possível usar a configuração central nem criar políticas de configuração em nenhuma região. As contas manterão as configurações que tinham antes de a região inicial ser alterada ou removida. É possível alterar essas configurações a qualquer momento, mas como a configuração central não é mais usada, as configurações devem ser modificadas separadamente em cada conta e região. É possível usar a configuração central e criar políticas de configuração novamente se uma nova região inicial for designada.

Para obter mais informações sobre a configuração central, consulte Como a configuração central funciona.

Habilitar a agregação entre regiões

Você deve habilitar a agregação entre regiões a partir da Região da AWS que você deseja designar como a Região de agregação.

Não é possível usar uma região desabilitada por padrão como região de agregação. Para obter uma lista de regiões desabilitadas por padrão, consulte Habilitar uma região no Referência geral da AWS.

Habilitar a agregação entre regiões (console)

Ao habilitar a agregação entre regiões, você escolhe suas regiões vinculadas. Você também escolhe se deseja vincular automaticamente novas regiões quando o Security Hub começa a ser compatível com elas e você as escolhe.

Habilitar a agregação entre regiões

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. Usando o Região da AWS seletor, faça login na região que você deseja usar como região de agregação.
3. No menu de navegação do Security Hub, escolha Configurações e, em seguida, Regiões.
4. Em Agregação de descoberta, escolha Configurar agregação de descoberta.

   Por padrão, a região de agregação é definida como Nenhuma região de agregação.
5. Em Região de agregação, selecione a opção para definir a região atual como a região de agregação.
6. Opcionalmente, em Regiões vinculadas, selecione as regiões das quais agregar dados.
7. Para agregar automaticamente dados de novas regiões na seção caso o Security Hub seja compatível com eles e você queira escolher esses dados, selecione Vincular regiões futuras.
8. Escolha Salvar.

Habilitando a agregação entre regiões (API do Security Hub) AWS CLI

É possível usar a API do Security Hub para habilitar a agregação entre regiões.

Para habilitar a agregação entre regiões a partir da API do Security Hub, você cria um agregador de descobertas. Você deve criar o agregador de descobertas da região que deseja usar como região de agregação.

Para criar o agregador de descoberta (API do Security Hub, AWS CLI)

- API do Security Hub: na região que você deseja usar como região de agregação, use a operação `CreateFindingAggregator`. Para as `RegionLinkingMode`, é possível escolher entre as opções a seguir:
  - `ALL_REGIONS` – O Security Hub agrega dados de todas as regiões. O Security Hub também agrega dados de novas regiões à medida que elas são compatíveis e você escolhe usá-las.

- `ALL_REGIONS_EXCEPT_SPECIFIED` – O Security Hub agrega dados de todas as regiões, exceto as que você deseja excluir. O Security Hub também agrega dados de novas regiões à medida que elas são compatíveis e você escolhe usá-las. Use `Regions` para fornecer a lista de regiões a serem excluídas da agregação.
- `SPECIFIED_REGIONS` – O Security Hub agrega dados de uma lista selecionada de regiões. O Security Hub não agrega dados automaticamente de novas regiões. Use `Regions` para fornecer a lista de regiões das quais agregar.

- AWS CLI: na linha de comando, execute o comando `create-finding-aggregator`. Separe cada região com um espaço.

```
aws securityhub create-finding-aggregator --region <aggregation Region> --region-
linking-mode ALL_REGIONS | ALL_REGIONS_EXCEPT_SPECIFIED | SPECIFIED_REGIONS --
regions <Region list>
```

  No exemplo a seguir, a agregação entre regiões está configurada para regiões selecionadas. A região de agregação é Leste dos EUA (Norte da Virgínia). As regiões vinculadas são Oeste dos EUA (Norte da Califórnia) e Oeste dos EUA (Oregon).

```
aws securityhub create-finding-aggregator --region us-east-1 --region-linking-mode
 SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Visualização de configurações de agregação entre regiões

É possível visualizar a configuração atual de agregação entre regiões de qualquer região. A configuração inclui a região de agregação, as regiões vinculadas e se as novas regiões devem ser vinculadas automaticamente.

Visualizar a configuração atual de agregação entre regiões (console)

A guia Regiões da página Configurações exibe a configuração atual de agregação entre regiões. É possível visualizar a configuração de qualquer região. As contas-membro também podem visualizar a configuração entre regiões que a conta de administrador configurou.

Se a agregação entre regiões não estiver habilitada, a guia Regiões exibirá a opção de habilitar a agregação entre regiões. Consulte the section called “Habilitar a agregação entre regiões”. Somente contas de administrador e contas autônomas podem habilitar a agregação entre regiões.

Se a agregação entre regiões estiver ativada, a guia Regiões exibirá as seguintes informações:

- A região de agregação
- Se você deseja agregar automaticamente descobertas, insights, status de controle e pontuações de segurança de novas regiões que o Security Hub é compatível e que você escolhe
- A lista de regiões vinculadas

Visualizando a configuração atual de agregação entre regiões (API do Security Hub,) AWS CLI

Você pode usar a API do Security Hub ou visualizar AWS CLI a configuração atual de agregação entre regiões. É possível visualizar a configuração de agregação entre regiões de qualquer região.

Visualizar a configuração atual de agregação entre regiões (API do Security Hub, AWS CLI)

- API do Security Hub: use a API `GetFindingAggregator`. Ao fazer a solicitação, você deve fornecer o ARN do agregador de descoberta. Para obter o ARN do agregador de descoberta, use o `ListFindingAggregators`.
- AWS CLI: na linha de comando, execute o comando `get-finding-aggregator`. Para obter o ARN do agregador de descoberta, use o `list-finding-aggregators`.

```
aws securityhub get-finding-aggregator --finding-aggregator-arn <finding aggregator
 ARN>
```

Atualizar a configuração de agregação entre regiões

É possível atualizar a configuração de agregação entre regiões para alterar a Regiões da AWS vinculada para a região de agregação atual. Você também pode alterar se deseja agregar automaticamente descobertas, insights, status de controle e pontuações de segurança de novas regiões.

As alterações na agregação entre regiões não serão implementadas em uma região de adesão até que a região seja habilitada em uma Conta da AWS. As regiões que AWS foram introduzidas em ou após 20 de março de 2019 são regiões optativas.

Quando você para de agregar dados de uma região vinculada, o Security Hub não remove nenhum dado agregado existente da região de agregação.

Você não pode usar o processo de atualização para alterar a região de agregação. Para alterar a região de agregação, você deve fazer o seguinte:

1. Interrompa a agregação entre regiões. Consulte the section called “Interromper a agregação entre regiões”.
2. Altere para a região da que você quer que seja a nova região de agregação.
3. Habilitar a agregação entre regiões. Consulte the section called “Habilitar a agregação entre regiões”.

Atualizar a configuração de agregação entre regiões (console)

Você deve atualizar a configuração de agregação entre regiões a partir da região de agregação atual.

Regiões da AWS Além da região de agregação, o painel Localizando agregação exibe uma mensagem informando que você deve editar a configuração na região de agregação. Escolha essa mensagem para exibir um link e navegar até a região de agregação.

Alterar as regiões vinculadas para a região de agregação atual

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. Mude para a região de agregação atual.
3. No menu de navegação do Security Hub, escolha Configurações e, em seguida, selecione Regiões.
4. Em Agregação de descoberta, escolha Editar.
5. Em Regiões vinculadas, atualize as regiões vinculadas selecionadas.
6. Se necessário, altere se a opção Vincular regiões futuras estiver selecionada. Essa configuração determina se o Security Hub vincula automaticamente novas regiões à medida que fica compatível com elas e você as escolhe.
7. Escolha Salvar.

Atualização da configuração de agregação entre regiões (API do Security Hub,) AWS CLI

Você pode usar a API do Security Hub ou atualizar AWS CLI a configuração de agregação entre regiões. Você deve atualizar a configuração de agregação entre regiões da região de agregação atual.

É possível alterar o modo de vinculação de regiões. Se o modo de vinculação for `ALL_REGIONS_EXCEPT_SPECIFIED` ou `SPECIFIED_REGIONS`, será possível alterar a lista de regiões excluídas ou incluídas.

Ao alterar a lista de regiões excluídas ou incluídas, você deve fornecer a lista completa com as atualizações. Por exemplo, suponha que você atualmente agrega descobertas do Leste dos EUA (Ohio) e queira agregar também descobertas do Oeste dos EUA (Oregon). Ao designar o `UpdateFindingAggregator`, você fornece uma lista de `Regions` que contém tanto o Leste dos EUA (Ohio) quanto o Oeste dos EUA (Oregon).

Para atualizar a agregação entre regiões (API do Security Hub,) AWS CLI

- API do Security Hub: use a operação API `UpdateFindingAggregator`. Para identificar o agregador de descoberta, você deve fornecer o ARN do agregador de descoberta. Para obter o ARN do agregador de descoberta, use o `ListFindingAggregators`.

  Você fornece o modo de vinculação de regiões e a lista atualizada de regiões excluídas ou incluídas.
- AWS CLI: na linha de comando, execute o comando `update-finding-aggregator`. Separe cada região com um espaço.

  ```
  aws securityhub update-finding-aggregator --region <aggregation Region> --finding-
  aggregator-arn <finding aggregator ARN> --region-linking-mode ALL_REGIONS |
   ALL_REGIONS_EXCEPT_SPECIFIED | SPECIFIED_REGIONS --regions <Region list>
  ```

  No exemplo a seguir, a configuração de agregação entre regiões é alterada a agregação de regiões selecionadas. O comando é executado na região de agregação atual, que é Leste dos EUA (Norte da Virgínia). As regiões vinculadas são Oeste dos EUA (Norte da Califórnia) e Oeste dos EUA (Oregon).

  ```
  aws securityhub update-finding-aggregator --region us-east-1 --finding-aggregator-arn
   arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-
  ```

```
a456-426652340000 --region-linking-mode SPECIFIED_REGIONS --regions us-west-1 us-
west-2
```

Interromper a agregação entre regiões

Interrompa a agregação entre regiões se você não quiser mais agregar dados ou se quiser alterar a região de agregação.

Quando você interrompe a agregação entre regiões, o Security Hub para de agregar dados. Ele não remove nenhum dado agregado existente da região de agregação.

Interromper a agregação entre regiões (console)

Você deve interromper a agregação entre regiões a partir da região de agregação atual.

Em regiões diferentes da região de agregação, o painel Agregação de descoberta exibe uma mensagem informando que você deve editar a configuração na região de agregação. Escolha essa mensagem para exibir um link e navegar até a região de agregação.

Interromper a agregação entre regiões

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. Mude para a região de agregação atual.
3. No menu de navegação do Security Hub, escolha Configurações e, em seguida, selecione Regiões.
4. Em Agregação de descoberta, escolha Editar.
5. Em Região de agregação, escolha Nenhuma região de agregação.
6. Escolha Salvar.
7. Na caixa de diálogo de confirmação, no campo de confirmação, digite **`Confirm`**.
8. Selecione a opção Confirmar.

Interrompendo a agregação entre regiões (API do Security Hub) AWS CLI

É possível usar a API do Security Hub para interromper a agregação entre regiões. Você deve interromper a agregação entre regiões a partir da região de agregação atual.

Para interromper a agregação entre regiões (API do Security Hub,) AWS CLI

- API do Security Hub: use a operação API `DeleteFindingAggregator`. Para identificar o agregador de descoberta para excluir, você deve fornecer o ARN do agregador de descoberta. Para obter o ARN do agregador de descoberta, use o `ListFindingAggregators`.
- AWS CLI: na linha de comando, execute o comando `delete-finding-aggregator`.

```
aws securityhub delete-finding-aggregator <finding aggregator ARN> --
region <aggregation Region>
```

Descobertas no AWS Security Hub

AWS O Security Hub elimina a complexidade de lidar com grandes volumes de descobertas de vários fornecedores. Ele reduz o esforço necessário para gerenciar e melhorar a segurança de todas as suas Contas da AWS, recursos e workloads.

O Security Hub recebe descobertas das origens a seguir.

- O Security Hub verifica os controles habilitados. Consulte the section called “Gerando e atualizando descobertas de controle”.
- Integrações com as Serviços da AWS que você habilita. Consulte the section called “AWS service (Serviço da AWS) integrações”.
- Integrações com produtos de terceiros habilitados. Consulte the section called “Integrações de produtos de terceiros”.
- Integrações personalizadas que você configura. Consulte the section called “Usar integrações de produtos personalizados”.

O Security Hub consome as descobertas usando um formato padrão de descobertas chamado AWS Security Finding Format. Para obter mais informações sobre o formato de descoberta, consulte the section called “Formato de descoberta”.

O Security Hub correlaciona as descobertas em produtos integrados para priorizar as mais importantes.

Os provedores de descoberta podem atualizar descobertas para refletir instâncias adicionais da descoberta. É possível atualizar as descobertas para fornecer detalhes sobre a investigação e seus resultados.

O Security Hub também permite agregar descobertas em todas as regiões, para que você possa visualizar todas as suas descobertas em um só lugar. Consulte Agregação entre regiões.

Tópicos

- AWS Formato de descoberta de segurança (ASFF)

Criando e atualizando descobertas no AWS Security Hub

Em AWS Security Hub, uma descoberta pode se originar de um dos seguintes tipos de provedores de busca.

- Um controle de segurança ativado no Security Hub
- Uma integração habilitada com outra AWS service (Serviço da AWS)
- Uma integração habilitada com um produto de terceiros

Depois que uma descoberta é criada, ela pode ser atualizada pelo provedor de descoberta ou pelo cliente.

- O provedor de descoberta usa a operação de API `BatchImportFindings` para atualizar as informações gerais sobre uma descoberta. Os provedores de descoberta só podem atualizar as descobertas que eles criaram.
- O cliente usa a operação da `BatchUpdateFindings`API para atualizar o status da investigação sobre uma descoberta. `BatchUpdateFindings`também pode ser usado por uma ferramenta de emissão de tíquetes, gerenciamento de incidentes, orquestração, remediação ou SIEM em nome do cliente.

  No console do Security Hub, os clientes podem visualizar detalhes de descobertas, gerenciar o status do fluxo de trabalho das descobertas e enviar descobertas para ações personalizadas. Consulte the section called “Tomar ação sobre descobertas ”.

O Security Hub também atualiza e exclui automaticamente as descobertas. Todas as descobertas serão excluídas automaticamente se não tiverem sido atualizadas nos últimos 90 dias.

Se você habilitar a agregação entre regiões, o Security Hub agregará automaticamente novas descobertas das regiões vinculadas à região de agregação. O Security Hub também replica as atualizações das descobertas. As atualizações que ocorrem nas regiões vinculadas são replicadas na região de agregação. As atualizações que ocorrem na região de agregação são replicadas na região vinculada. Para obter mais informações sobre agregação entre regiões, consulte Agregação entre regiões.

Tópicos

Usar BatchImportFindings para criar e atualizar descobertas

Os provedores de descoberta usam a operação de API `BatchImportFindings` para criar descobertas e atualizar informações sobre as descobertas que eles criaram. Eles não podem atualizar descobertas que não criaram.

Clientes, SIEMs, ferramentas de emissão de bilhetes e ferramentas SOAR usam `BatchUpdateFindings`para fazer atualizações relacionadas à investigação de descobertas de fornecedores. Consulte the section called “Usar o BatchUpdateFindings”.

Sempre que AWS Security Hub recebe uma `BatchImportFindings` solicitação para criar ou atualizar uma descoberta, ela gera automaticamente um Security Hub Findings - Importedevento na Amazon EventBridge. Consulte the section called “Resposta e remediação automatizadas”.

Requisitos para contas e tamanho do lote

`BatchImportFindings` deve ser um dos seguintes:

- A conta da AWS associada com as descobertas. O identificador da conta associada é o valor do atributo `AwsAccountId` para a descoberta.
- Uma conta que está na lista de permissões para uma integração oficial de parceiros do Security Hub.

O Security Hub só pode aceitar atualizações de descobertas para contas que tenham o Security Hub habilitado. O provedor de descoberta também deve estar habilitado. Se o Security Hub estiver desabilitado ou se a integração do provedor de descoberta não estiver habilitada, as descobertas serão retornadas na lista `FailedFindings`, com um erro `InvalidAccess`.

`BatchImportFindings` aceita até 100 descobertas por lote, até 240 KB por descoberta e até 6 MB por lote. O limite da taxa de controle de utilização é de 10 TPS por conta por região, com uma explosão de 30 TPS.

Determinar se uma descoberta deve ser criada ou atualizada

Para determinar se deseja criar ou atualizar uma descoberta, o Security Hub verifica o campo `ID`. Se o valor de `ID` não corresponder a uma descoberta existente, uma descoberta será criada.

Se `ID` corresponder a uma descoberta existente, o Security Hub verifica o campo `UpdatedAt` para a atualização.

- Se `UpdatedAt` na atualização corresponder ou ocorrer antes de `UpdatedAt` na descoberta existente, a atualização será ignorada.
- Se `UpdatedAt` na atualização ocorrer após `UpdatedAt` na descoberta existente, ela será atualizada.

Atributos restritos para BatchImportFindings

Para uma descoberta existente, os provedores de localização não podem usar `BatchImportFindings` para atualizar os atributos e objetos a seguir. Esses atributos só podem ser atualizados usando `BatchUpdateFindings`.

- `Note`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

O Security Hub ignora qualquer conteúdo fornecido em uma `BatchImportFindings` solicitação para esses atributos e objetos. Os clientes, ou outros provedores que atuam em seu nome, usam `BatchUpdateFindings` para atualizá-los.

Usar o FindingProviderFields

Encontrar provedores também não deve ser usado `BatchImportFindings` para atualizar os seguintes atributos.

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

Em vez disso, os provedores de descoberta usam o objeto `FindingProviderFields` para fornecer valores para esses atributos.

Exemplo

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

Para solicitações `BatchImportFindings`, o Security Hub manipula valores nos atributos de nível superior e no `FindingProviderFields` da seguinte forma.

(Preferencial) O **`BatchImportFindings`** fornece um valor para um atributo em **`FindingProviderFields`**, mas não fornece um valor para o atributo de nível superior correspondente.

Por exemplo, o `BatchImportFindings` fornece `FindingProviderFields.Confidence`, mas não fornece `Confidence`. Essa é a opção preferida para solicitações `BatchImportFindings`.

O Security Hub atualiza o valor do atributo no `FindingProviderFields`.

Ele replica o valor para o atributo de nível superior somente se o atributo ainda não tiver sido atualizado pelo. `BatchUpdateFindings`

O **`BatchImportFindings`** fornece um valor para um atributo de nível superior, mas não fornece um valor para o atributo correspondente em **`FindingProviderFields`**.

Por exemplo, o `BatchImportFindings` fornece `Confidence`, mas não fornece `FindingProviderFields.Confidence`.

O Security Hub usa o valor para atualizar o atributo no `FindingProviderFields`. Ele sobrescreve qualquer valor existente.

O Security Hub atualiza o atributo de nível superior somente se o atributo ainda não tiver sido atualizado por `BatchUpdateFindings`.

`BatchImportFindings` fornece um valor para um atributo de nível superior e para o atributo correspondente em **`FindingProviderFields`**.

Por exemplo, `BatchImportFindings` fornece ambos `Confidence` e `FindingProviderFields.Confidence`.

Para uma nova descoberta, o Security Hub usa o valor em `FindingProviderFields` para preencher o atributo de nível superior e o atributo correspondente em `FindingProviderFields`. Ele não usa o valor do atributo de nível superior fornecido.

Para uma descoberta existente, o Security Hub usa os dois valores. Entretanto, ele atualiza o atributo de nível superior somente se o atributo ainda não tiver sido atualizado por `BatchUpdateFindings`.

Usando o batch-import-findings comando do AWS CLI

No AWS Command Line Interface, você usa o `batch-import-findings`comando para criar ou atualizar descobertas.

Você fornece cada descoberta como um objeto JSON.

Exemplo

```
aws securityhub batch-import-findings --findings
    [{
        "AwsAccountId": "123456789012",
        "CreatedAt": "2019-08-07T17:05:54.832Z",
        "Description": "Vulnerability in a CloudTrail trail",
        "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0/rule/2.2",
        "Id": "Id1",
        "ProductArn": "arn:aws:securityhub:us-west-1:123456789012:product/123456789012/
default",
        "Resources": [
            {
                "Id": "arn:aws:cloudtrail:us-west-1:123456789012:trail/TrailName",
                "Partition": "aws",
                "Region": "us-west-1",
```

```
                "Type": "AwsCloudTrailTrail"
            }
        ],
        "SchemaVersion": "2018-10-08",
        "Title": "CloudTrail trail vulnerability",
        "UpdatedAt": "2020-06-02T16:05:54.832Z",
        "Types": [
            "Software and Configuration Checks/Vulnerabilities/CVE"
        ],
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "0"
        }
    }]'
```

Usar BatchUpdateFindings para atualizar uma descoberta

A ação `BatchUpdateFindings` é usada para atualizar as informações relacionadas ao processamento de descobertas de um cliente por provedores de descobertas. Ele pode ser usado por um cliente ou por uma ferramenta de SIEM, emissão de bilhetes, gerenciamento de incidentes ou SOAR que trabalha em nome de um cliente. Você pode usar `BatchUpdateFindings` para atualizar campos específicos no Formato AWS de descoberta de segurança (ASFF).

Você não pode usar `BatchUpdateFindings` para criar novas descobertas. É possível usá-lo para atualizar até 100 descobertas por vez.

Sempre que o Security Hub recebe uma `BatchUpdateFindings` solicitação para atualizar uma descoberta, ele gera automaticamente um Security Hub Findings - Importedevento na Amazon EventBridge. Consulte the section called “Resposta e remediação automatizadas”.

`BatchUpdateFindings`não altera o `UpdatedAt` campo da descoberta. `UpdatedAt`reflete apenas a atualização mais recente do provedor de busca.

Campos disponíveis para BatchUpdateFindings

As contas de administrador podem usar >`BatchUpdateFindings` para atualizar descobertas para sua conta ou para suas contas-membro. As contas-membro podem usar >`BatchUpdateFindings` para atualizar descobertas para sua conta.

Os clientes só podem usar > `BatchUpdateFindings` para atualizar os seguintes campos e objetos.

- `Confidence`
- `Criticality`
- `Note`
- `RelatedFindings`
- `Severity`
- `Types`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Por padrão, as contas de administrador e membro têm acesso a todos os campos e valores de campo acima. O Security Hub também fornece chaves de contexto para permitir que você restrinja o acesso a campos e valores de campo.

Por exemplo, é possível permitir que somente as contas dos membros definam `Workflow.Status` como `RESOLVED`. Ou talvez você não queira permitir que as contas dos membros alterem `Severity.Label`.

Como configurar o acesso ao BatchUpdateFindings

É possível configurar políticas do IAM para restringir o acesso ao uso de `BatchUpdateFindings` para atualizar campos e valores de campo.

Em uma declaração para restringir o acesso ao `BatchUpdateFindings`, use os seguintes valores:

- `Action` é `securityhub:BatchUpdateFindings`
- `Effect` é `Deny`
- Para `Condition`, é possível negar uma solicitação `BatchUpdateFindings` com base no seguinte:
  - A descoberta inclui um campo específico.
  - A descoberta inclui um valor de campo específico.

Chaves de condição

Essas são as principais condições para restringir o acesso ao `BatchUpdateFindings`.

Campo do ASFF

A principal condição para um campo do ASFF é a seguinte:

```
securityhub:ASFFSyntaxPath/<fieldName>
```

Substitua *<fieldName>* pelo campo do ASFF. Ao configurar o acesso ao `BatchUpdateFindings`, inclua um ou mais campos do ASFF específicos em sua política do IAM em vez de um campo de nível principal. Por exemplo, para restringir o acesso ao campo `Workflow.Status`, você deve incluir `securityhub:ASFFSyntaxPath/Workflow.Status` em sua política em vez do campo de nível principal `Workflow`.

Proibir atualizações em um campo

Para impedir que um usuário faça qualquer atualização em um campo específico, use uma condição como esta:

```
 "Condition": {
                "Null": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "false"
               }
}
```

Por exemplo, a declaração a seguir indica que `BatchUpdateFindings` não pode ser usado para atualizar o status do fluxo de trabalho.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
        "Null": {
            "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
        }
    }
}
```

Proibir valores de campo específicos

Para impedir que um usuário configure um campo para um valor específico, use uma condição como esta:

```
"Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
                }
}
```

Por exemplo, a declaração a seguir indica que `BatchUpdateFindings` não pode ser usado para configurar `Workflow.Status` para `SUPPRESSED`.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
}
```

Você também pode fornecer uma lista de valores que não são permitidos.

```
 "Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
 "<fieldValue2>", "<fieldValuen>" ]
                }
}
```

Por exemplo, a declaração a seguir indica que `BatchUpdateFindings` não pode ser usado para configurar `Workflow.Status` para `RESOLVED` ou `SUPPRESSED`.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
```

```
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": [
            "RESOLVED",
            "NOTIFIED"
        ]
    }
}
```

Usando o batch-update-findings comando do AWS CLI

No AWS Command Line Interface, você usa o `batch-update-findings`comando para atualizar as descobertas.

Para cada descoberta a ser atualizada, você fornece o ID da descoberta e o ARN do produto que gerou a descoberta.

```
--finding-identifiers ID="<findingID1>",ProductArn="<productARN>"
 ID="<findingID2>",ProductArn="<productARN2>"
```

Quando você fornece os atributos a serem atualizados, é possível usar um formato JSON ou um formato de atalho.

Aqui está um exemplo de uma atualização no objeto `Note` que usa o formato JSON:

```
--note '{"Text": "Known issue that is not a risk.", "UpdatedBy": "user1"}'
```

Aqui está a mesma atualização que usa o formato de atalho:

```
--note Text="Known issue that is not a risk.",UpdatedBy="user1"
```

A Referência de AWS CLI Comandos fornece o JSON e a sintaxe de atalho para cada campo.

O exemplo > `batch-update-findings` a seguir atualiza duas descobertas para adicionar uma nota, alterar o rótulo de severidade e resolvê-las.

```
aws securityhub batch-update-findings --finding-identifiers Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-2::product/aws/securityhub" Id="arn:aws:securityhub:us-
```

```
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" --note '{"Text": "Known issue that is not a
 risk.", "UpdatedBy": "user1"}' --severity '{"Label": "LOW"}' --workflow '{"Status":
 "RESOLVED"}'
```

Esse é o mesmo exemplo, mas usa os atalhos em vez de JSON.

```
aws securityhub batch-update-findings --finding-identifiers Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" Id="arn:aws:securityhub:us-
west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",ProductArn="arn:aws:securityhub:us-
west-1::product/aws/securityhub" --note Text="Known issue that is not a
 risk.",UpdatedBy="user1" --severity Label="LOW" --workflow Status="RESOLVED"
```

Gerenciando e revisando detalhes e histórico de busca

Há várias maneiras de ver as listas de busca no AWS Security Hub console:

- Página de descobertas — Exibe uma lista abrangente de descobertas de todos os controles habilitados e integrações de produtos. Por padrão, as descobertas ativas com um status de `NOTIFIED` fluxo de trabalho `NEW` ou são mostradas.
- Página de detalhes do controle — Exibe uma lista das descobertas que foram geradas nas últimas 24 horas para um controle específico.
- Página de insights — Exibe uma lista de descobertas para uma visão correspondente. Um insight é uma coleção de descobertas específicas. Para ter mais informações, consulte the section called “Visualizar resultados e descobertas de insight”.
- Página de integrações — Exibe uma lista das descobertas geradas por um produto integrado AWS service (Serviço da AWS) ou de terceiros.

Você pode filtrar e agrupar as descobertas nessas listas para se concentrar em tipos específicos de descobertas. Você também pode selecionar uma descoberta específica nas páginas anteriores para ver detalhes sobre ela.

Para ver uma lista de descobertas de forma programática, use a `GetFindings`operação da API do Security Hub. Você pode incluir filtros para recuperar tipos específicos de descobertas.

Se você habilitar a agregação entre regiões, poderá recuperar status de controle, pontuações de segurança, insights e descobertas de todas as regiões. Na região de agregação, a localização de dados inclui dados da região de agregação e das regiões vinculadas. Em outras regiões, a localização de dados é específica somente para aquela região. Para obter informações sobre como configurar a agregação entre regiões, consulte. Agregação entre regiões

Filtragem e agrupamento de descobertas (console)

Quando você exibe uma lista de descobertas na página Descobertas, na página Integrações ou na página Insights do console do Security Hub, a lista é pré-filtrada com base no estado do registro e no status do fluxo de trabalho. Além dos filtros para um insight ou uma integração.

O estado do registro indica se uma descoberta está ativa ou arquivada. Por padrão, uma lista de descobertas mostra somente as descobertas ativas. Uma descoberta pode ser arquivada pelo provedor da descoberta. AWS Security Hub também arquiva automaticamente as descobertas de controle se o recurso associado for excluído.

O status do fluxo de trabalho indica o status de uma investigação sobre uma descoberta. Por padrão, uma lista de busca mostra somente descobertas com um status de fluxo de trabalho de `NEW` ou `NOTIFIED`. Você pode atualizar o status do fluxo de trabalho de uma descoberta.

Se você ativou a agregação de descobertas e está conectado à região de agregação, você pode filtrar as descobertas por região nas páginas Descobertas e Insights.

Para obter informações sobre como trabalhar com descobertas de controle, consultethe section called “Filtrar e classificar descobertas”. As informações nesta página se aplicam às listas de descobertas nas páginas Descobertas, Insights e Integrações.

Adicionar filtros

Para alterar o escopo da lista, é possível adicionar filtros a ela.

É possível filtrar por até 10 atributos. Para cada atributo, é possível fornecer até 20 valores de filtro.

Ao filtrar a lista de descobertas, o Security Hub aplica a lógica E ao conjunto de filtros. Em outras palavras, uma descoberta só será correspondente se corresponder a todos os filtros fornecidos. Por exemplo, se você adicionar GuardDuty como filtro para o nome do produto e `AwsS3Bucket` como filtro para o tipo de recurso, as descobertas correspondentes deverão corresponder a esses dois critérios.

Entretanto, o Security Hub aplica a lógica OU a filtros que usam o mesmo atributo, mas valores diferentes. Por exemplo, você adiciona ambos GuardDuty e o Amazon Inspector como valores de filtro para o nome do produto. Nesse caso, uma descoberta corresponde se foi gerada por um GuardDuty ou pelo Amazon Inspector.

Como adicionar um filtro à lista de descobertas

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. Para exibir uma lista de descobertas, execute um destes procedimentos:
   - No painel de navegação do Security Hub, selecione Descobertas.
   - No painel de navegação do Security Hub, selecione Insights. Escolha um insight. Em seguida, na lista de resultados, escolha um resultado de insight.
   - No painel de navegação do Security Hub, selecione Integrações. Escolha Ver descobertas para obter uma integração.
3. Na caixa Adicionar filtros, em Filtros, escolha um filtro.

   Quando você filtra por nome da empresa ou nome do produto, o console usa o nível superior `CompanyName` e `ProductName` os campos. A API usa os valores que estão em `ProductFields`.
4. Selecione o tipo de correspondência do filtro.

   Para um filtro de string, é possível escolher as seguintes opções de comparação:

   - é: encontre um valor que corresponda exatamente ao valor do filtro.
   - começa com: encontre um valor que comece com o valor do filtro.
   - não é: encontre um valor que não corresponda ao valor do filtro.
   - não começa com: encontre um valor que não comece com o valor do filtro.

   Para um filtro numérico, é possível escolher se será fornecido um único número (Simples) ou um intervalo de números (Intervalo).

   Para um filtro de data e hora, é possível escolher se será fornecido um período a partir da data atual (Janela de rolagem) ou de um intervalo de datas específico (Intervalo fixo).

   Adicionar vários filtros tem as seguintes interações:

- Filtros é e começa com unidos por OR. Um valor corresponde se ele contiver algum dos valores do filtro. Por exemplo, se você especificar que o Rótulo de severidade é CRÍTICO e o Rótulo de severidade é ALTO, os resultados incluirão as descobertas de severidade crítica e alta.
- Os filtros não é e não começa com são unidos por E. Um valor corresponde apenas se não contiver algum dos valores do filtro. Por exemplo, se você especificar que o rótulo de gravidade não é BAIXO e o rótulo de gravidade não é MÉDIO, os resultados não incluirão resultados de gravidade baixa ou média.

Se você tiver um filtro é em um campo, você não pode ter um filtro não é ou não começa com um filtro no mesmo campo.

5. Especifique o valor do filtro.

   Para filtros de string, o valor do filtro diferencia maiúsculas de minúsculas.

   Por exemplo, para descobertas do Security Hub, o Nome do produto é Security Hub. Se você usar o operador EQUALS para ver as descobertas do Security Hub, será necessário inserir **`Security Hub`** como o valor do filtro. Se você inserir **`security hub`**, não será exibida nenhuma descoberta.

   Da mesma forma, se você usar o operador PREFIX e inserir **`Sec`**, as descobertas do Security Hub serão exibidas. Se você inserir **`sec`**, nenhuma descoberta do Security Hub será exibida.

6. Escolha Aplicar.

Agrupar descobertas

Além de alterar os filtros, é possível agrupar as descobertas com base nos valores de um atributo selecionado.

Quando você agrupa as descobertas, a lista de descobertas é substituída por uma lista de valores para o atributo selecionado nas descobertas correspondentes. Para cada valor, a lista exibe o número de descobertas que correspondem aos outros critérios de filtro.

Por exemplo, se você agrupar as descobertas por Conta da AWS ID, verá uma lista de identificadores de conta, com o número de descobertas correspondentes para cada conta.

Observe que o Security Hub pode exibir somente 100 valores. Se houver mais de 100 valores de agrupamento, você verá somente os 100 primeiros.

Quando você escolhe um valor de atributo, é exibida a lista de descobertas correspondentes para esse valor de campo.

Como agrupar as descobertas em uma lista de descobertas

1. Na lista de descobertas, escolha a caixa Adicionar filtros.
2. Em Agrupamento, escolha Agrupar por.
3. Na lista, selecione o atributo a ser usado para o agrupamento.
4. Escolha Aplicar.

Alterar um valor de filtro ou um atributo de agrupamento

Para um filtro existente, é possível alterar o valor do filtro. Também é possível alterar o atributo de agrupamento.

Por exemplo, é possível alterar o filtro de Record state (Estado do registro) para procurar descobertas `ARCHIVED` em vez de descobertas `ACTIVE`.

Para editar um filtro ou atributo de agrupamento

1. Em uma lista de descoberta filtrada, escolha o atributo de filtro ou agrupamento.
2. Em Agrupar por, escolha o novo atributo e, em seguida, escolha Aplicar.
3. Para um filtro, selecione o novo valor e Aplicar.

Excluir um atributo de filtro ou agrupamento

Para excluir um atributo de filtro ou agrupamento, selecione o ícone x.

A lista é atualizada automaticamente para refletir a alteração. Quando você remove o atributo de agrupamento, a lista muda da lista de valores de campo de volta para uma lista de descobertas.

Informações de busca disponíveis

Você pode obter vários detalhes das descobertas no console do Security Hub ou chamando a GetFindingsoperação da API do Security Hub. Aqui está uma lista parcial dos tipos de detalhes de descoberta que você pode obter.

- Metadados do aplicativo — Fornece o nome de recurso da Amazon (ARN) do aplicativo envolvido na descoberta se você criou um aplicativo e adicionou a tag do aplicativo AWS a ele. Recomendamos criar aplicativos em AWS Service Catalog AppRegistry.
- Histórico de descobertas — Fornece o histórico da descoberta nos últimos 90 dias.
- Encontrando uma investigação no Detective (somente console) — fornece um link para investigar mais detalhadamente uma descoberta no Detective usando ferramentas automatizadas de coleta de registros, análise de segurança e AWS service (Serviço da AWS) exploração de recursos. Essas informações só serão incluídas nas descobertas do Security Hub recebidas de outras pessoas Serviços da AWS se você ativar o Detective.
- Campos de localização do provedor — exibe os valores do provedor de busca quanto à confiança, criticidade, descobertas relacionadas, gravidade e tipo de descoberta.
- Parâmetros — Mostra os valores dos parâmetros atuais para um controle de segurança. O Security Hub usa esses valores de parâmetros ao realizar verificações de segurança do controle.
- Remediação — fornece um link para as instruções para remediar descobertas de controle malsucedidas.
- Recurso — Fornece informações sobre o AWS recurso envolvido em uma descoberta.
- Tags de recursos — Fornece informações sobre a chave e o valor da tag para os recursos envolvidos em uma descoberta. Você pode marcar recursos que são compatíveis com a `GetResources` operação da API de AWS Resource Groups marcação. Para obter mais informações sobre a inclusão de tags de recursos nas descobertas, consulteTags.
- Tipos e descobertas relacionadas — Contém informações sobre o tipo de descoberta.
- Detalhes da vulnerabilidade — Informações sobre uma vulnerabilidade detectada em uma descoberta e em pacotes afetados. Esses detalhes estão disponíveis se você habilitar o Amazon Inspector para as descobertas que o Amazon Inspector envia para o Security Hub.

Analise as seções a seguir para entender como acessar esses detalhes para uma descoberta.

Analisando o histórico de descobertas

O histórico de descobertas é um recurso do Security Hub que permite rastrear as alterações feitas em uma descoberta nos últimos 90 dias. Ele está disponível para descobertas ativas e arquivadas. O histórico de descobertas fornece uma trilha imutável das alterações feitas em uma descoberta ao longo do tempo, incluindo qual foi a alteração, quando ela ocorreu e por qual usuário.

Em particular, é possível acompanhar as alterações feitas nos campos no AWS Formato de descoberta de segurança (ASFF). O Security Hub rastreia as alterações que você faz manualmente e com regras de automação.

O histórico de localização está disponível no console do Security Hub, na API AWS CLI e.

Se você estiver conectado a uma conta de administrador do Security Hub, poderá obter o histórico de descobertas da conta do administrador e de todas as contas dos membros.

Escolha seu método preferido e siga as etapas para revisar o histórico de descobertas.

Security Hub console

Analisando o histórico de descobertas

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação à esquerda, escolha Descobertas.
3. Selecione uma descoberta. No painel exibido, escolha a guia Histórico.

Security Hub API

Analisando o histórico de descobertas

1. Execute ou GetFindings, se estiver usando o AWS CLI, execute o get-findingscomando. usando filtros apropriados conforme necessário, para identificar a descoberta da qual você deseja visualizar o histórico. A resposta da API fornecerá o `ProductArn` e `Id` para a descoberta. Você precisa dos valores desses campos na terceira etapa.
2. Execute ou GetFindingHistory, se estiver usando o AWS CLI, execute o get-finding-historycomando.
3. Identifique a descoberta da qual você deseja obter o histórico com os campos `Id` e `ProductArn`. Consulte mais informações sobre esses campos em AwsSecurityFindingIdentifier. Você só pode obter o histórico de uma descoberta por solicitação.
4. Forneça valores para`StartTime`. e `EndTime` para limitar o histórico de descobertas a um período de tempo específico.
5. Forneça um valor para `MaxResults` para limitar o histórico de descobertas a um número específico de resultados. Se não for fornecida, a resposta da API retornará os primeiros 100 resultados do histórico de descobertas.

6. Forneça um valor para `NextToken` para visualizar os próximos 100 resultados (se aplicável) de uma descoberta. Em sua solicitação inicial de API, o valor de `NextToken` deveria serNULL.

O comando CLI a seguir recupera o histórico da descoberta especificada. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha “barra invertida (\)” para melhorar a legibilidade.

```
$ aws securityhub get-finding-history \
--region us-west-2 \
--finding-identifier Id="a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-2:123456789012:product/123456789012/default" \
--max-results 2 \
--start-time "2021-09-30T15:53:35.573Z" \
--end-time "2021-09-31T15:53:35.573Z"
```

Analisando os detalhes da descoberta

Escolha seu método preferido e siga as etapas para ver os detalhes de busca no Security Hub.

Security Hub console

Analisando os detalhes da descoberta

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. Para exibir uma lista de descobertas, execute uma das seguintes ações:
   - No painel de navegação do Security Hub, selecione Descobertas. Adicione filtros de pesquisa conforme necessário para restringir a lista de descobertas.
   - No painel de navegação do Security Hub, selecione Insights. Escolha um insight. Em seguida, na lista de resultados, escolha um resultado de insight.
   - No painel de navegação do Security Hub, selecione Integrações. Escolha Ver descobertas para obter uma integração.
3. Selecione um título de descoberta.
4. No painel de detalhes da descoberta, você pode realizar ações adicionais da seguinte forma:

- Para exibir o JSON completo da descoberta, selecione o ID da descoberta. Em Finding JSON, baixe o Finding JSON.
- Para descobertas baseadas em AWS Config regras, para exibir uma lista das regras aplicáveis, escolha Regras.
- Escolha Investigar com Macie para investigar dados confidenciais descobertos na descoberta no console do Macie. Essa opção só está disponível se você ativar o Amazon Macie e seu recurso automatizado de descoberta de dados confidenciais.
- Escolha Recursos para visualizar informações sobre o recurso envolvido em uma descoberta.
- Escolha Investigar no Amazon Detective para investigar a descoberta no console do Detective. Essa opção só está disponível se você ativar o Amazon Detective.
- Escolha a guia Histórico para ver até 90 dias do histórico de buscas.

> **Note**
>
> A parte superior do painel de detalhes da descoberta contém informações gerais sobre a descoberta, incluindo a conta, a severidade, as datas e o status. Se você se integra AWS Organizations e a conta na qual está conectado for uma conta de membro da organização, o painel de detalhes incluirá o nome da conta. Para contas-membro que são convidados manualmente em vez de por meio da integração com o Organizations, o painel de detalhes inclui apenas o ID da conta.

Security Hub API

Analisando os detalhes da descoberta

Use a `GetFindings`operação da API do Security Hub ou, se estiver usando a AWS CLI, execute o comando get-findings.

Você pode fornecer um ou mais valores para o `Filters` parâmetro para restringir as descobertas que você deseja recuperar.

Se o volume de resultados for muito grande, você poderá usar o `MaxResults` parâmetro para limitar as descobertas a um número especificado e o `NextToken` parâmetro para paginar as

descobertas. Use o `SortCriteria` parâmetro para classificar as descobertas por um campo específico.

Se você ativou a agregação entre regiões e invocou essa operação a partir da região de agregação, os resultados incluem descobertas da agregação e regiões vinculadas.

O comando CLI a seguir recupera as descobertas que correspondem aos filtros fornecidos e as classifica em ordem decrescente do campo. `LastObservedAt` Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha "barra invertida (\)" para melhorar a legibilidade.

```
$ aws securityhub get-findings \
--filters '{"GeneratorId":[{"Value": "aws-
foundational","Comparison":"PREFIX"}],"WorkflowStatus": [{"Value":
 "NEW","Comparison":"EQUALS"}],"Confidence": [{"Gte": 85}]}' --sort-criteria
 '{"Field": "LastObservedAt","SortOrder": "desc"}' --page-size 5 --max-items 100
```

PowerShell

Analisando os detalhes da descoberta

1. Use o cmdlet `Get-SHUBFinding`.
2. Opcionalmente, preencha o parâmetro `Filter` para restringir as descobertas que você deseja recuperar.

Exemplo

```
Get-SHUBFinding -Filter @{AwsAccountId =
 [Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =
 "XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =
 "EQUALS"; Value = 'FAILED'}}
```

> **Note**
>
> Quando você filtra as descobertas por `CompanyName` ou`ProductName`, o Security Hub usa os valores que fazem parte do objeto `ProductFields` ASFF. O Security Hub não usa o nível superior `CompanyName` e `ProductName` os campos.

Tomando medidas com base nas descobertas em AWS Security Hub

AWS Security Hub permite que você acompanhe o status atual de sua investigação sobre uma descoberta.

Você também pode enviar descobertas para ações personalizadas para processamento.

Tópicos

Definir o status do fluxo de trabalho das descobertas

O status do fluxo de trabalho rastreia o progresso da investigação sobre uma descoberta. O status do fluxo de trabalho é específico para uma descoberta individual. Isso não afeta a geração de novas descobertas. Por exemplo, definir o status do fluxo de trabalho de uma descoberta como `SUPPRESSED` ou `RESOLVED` não AWS Security Hub impede a geração de uma nova descoberta para o mesmo problema.

O status do fluxo de trabalho pode ter um dos valores a seguir:

`NEW`

O estado inicial de uma descoberta, antes de ser revisada.

As descobertas que são ingeridas de forma integrada Serviços da AWS, como AWS Config, têm `NEW` como status inicial.

O Security Hub também redefine o status do fluxo de trabalho de `NOTIFIED` ou `RESOLVED` para `NEW` nos seguintes casos:

- `RecordState` é alterado de `ARCHIVED` para `ACTIVE`.
- `Compliance.Status` é alterado de `PASSED` para `FAILED`, `WARNING`, ou `NOT_AVAILABLE`.

Essas alterações implicam que uma investigação adicional é necessária.

`NOTIFIED`

Indica que você notificou o proprietário do recurso sobre o problema de segurança. É possível usar esse status quando você não é o proprietário do recurso e precisa de intervenção do proprietário do recurso para resolver um problema de segurança.

Se uma das situações a seguir ocorrer, o status do fluxo de trabalho será alterado automaticamente de `NOTIFIED` para `NEW`:

- `RecordState` é alterado de `ARCHIVED` para `ACTIVE`.
- `Compliance.Status` é alterado de `PASSED` para `FAILED`, `WARNING`, ou `NOT_AVAILABLE`.

`SUPPRESSED`

Indica que você revisou a descoberta e não acredita que nenhuma ação seja necessária.

O status do fluxo de trabalho de uma descoberta `SUPPRESSED` não muda se `RecordState` mudar de `ARCHIVED` para `ACTIVE`.

`RESOLVED`

A descoberta foi revisada e corrigida e agora é considerada resolvida.

A descoberta permanece `RESOLVED`, a menos que uma das seguintes condições ocorra:

- `RecordState` é alterado de `ARCHIVED` para `ACTIVE`.
- `Compliance.Status` é alterado de `PASSED` para `FAILED`, `WARNING`, ou `NOT_AVAILABLE`.

Nesses casos, o status do fluxo de trabalho é automaticamente redefinido para `NEW`.

Para descobertas de controles, se `Compliance.Status` for `PASSED`, o Security Hub definirá automaticamente o status do fluxo de trabalho como `RESOLVED`.

Definir o status do fluxo de trabalho das descobertas

Escolha seu método preferido e siga as etapas para definir o status do fluxo de trabalho de uma ou mais descobertas.

Para atualizar automaticamente o status do fluxo de trabalho de descobertas específicas, consulte Regras de automação.

Security Hub console

Para definir o status do fluxo de trabalho das descobertas

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. Para exibir uma lista de descobertas, execute um destes procedimentos:
   - No painel de navegação do Security Hub, selecione Descobertas.
   - No painel de navegação do Security Hub, selecione Insights. Escolha um insight. Em seguida, na lista de resultados, escolha um resultado de insight.
   - No painel de navegação do Security Hub, selecione Integrações. Escolha Ver descobertas para obter uma integração.
   - No painel de navegação do Security Hub, selecione Padrões de segurança. Escolha Exibir resultados para exibir uma lista de controles. Em seguida, selecione um controle para ver uma lista das descobertas desse controle.
3. Na lista de descobertas, marque a caixa de seleção para cada descoberta que você deseja atualizar.
4. No topo da lista, em Status do fluxo de trabalho, escolha o status.
5. Na caixa de diálogo Definir status do fluxo de trabalho, forneça uma nota opcional que detalha o motivo da atualização do status do fluxo de trabalho. Escolha Definir status.

Security Hub API

Invoque a API `BatchUpdateFindings`. Forneça o ID da descoberta e o ARN do produto que gerou a descoberta. É possível obter esses detalhes invocando a API `GetFindings`.

AWS CLI

Execute o comando `batch-update-findings`. Forneça o ID da descoberta e o ARN do produto que gerou a descoberta. É possível obter esses detalhes executando o comando do `get-findings`.

```
batch-update-findings --finding-identifiers
 Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

Exemplo

```
aws securityhub batch-update-findings --finding-identifiers
 Id="arn:aws:securityhub:us-west-1:123456789012:subscription/
pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --
workflow Status="RESOLVED"
```

Enviar descobertas para uma ação personalizada

Você pode criar ações AWS Security Hub personalizadas para automatizar o Security Hub com a Amazon EventBridge. Para ações personalizadas, o tipo de evento é Security Hub Findings - Custom Action.

Para obter mais informações e etapas detalhadas sobre como criar ações personalizadas, consulte the section called “Resposta e remediação automatizadas”.

Depois de configurar uma ação personalizada, será possível enviar descobertas para ela.

Como enviar descobertas para uma ação personalizada (console)

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. Para exibir uma lista de descobertas, execute um destes procedimentos:
   - No painel de navegação do Security Hub, selecione Descobertas.
   - No painel de navegação do Security Hub, selecione Insights. Escolha um insight. Em seguida, na lista de resultados, escolha um resultado de insight.
   - No painel de navegação do Security Hub, selecione Integrações. Escolha Ver descobertas para obter uma integração.
   - No painel de navegação do Security Hub, selecione Padrões de segurança. Escolha Exibir resultados para exibir uma lista de controles. Em seguida, escolha o nome do controle.
3. Na lista de descobertas, marque a caixa de seleção para cada descoberta a ser enviada para a ação personalizada.

   É possível enviar até 20 descobertas por vez.
4. Em Ações, escolha a ação personalizada.

AWS Formato de descoberta de segurança (ASFF)

AWS O Security Hub consome, agrega, organiza e prioriza as descobertas dos serviços de AWS segurança e das integrações de produtos de terceiros. O Security Hub processa essas descobertas usando um formato padrão de descobertas chamado AWS Security Finding Format (ASFF), que elimina a necessidade de esforços demorados de conversão de dados. Ele correlaciona as descobertas ingeridas nos produtos para priorizar as mais importantes.

Tópicos

AWS Sintaxe do Security Finding Format (ASFF)

Esta página fornece um resumo completo do JSON para uma descoberta no AWS Security Finding Format (ASFF). O formato é derivado do Esquema JSON. Escolha um nome de objeto vinculado para ver um exemplo de descoberta desse objeto. É possível comparar suas descobertas do Security Hub com os recursos e exemplos mostrados aqui para ajudá-lo a interpretar suas descobertas.

Para ver as descrições dos atributos ASFF necessários, consultethe section called “Atributos de nível superior necessários”.

Para ver as descrições dos atributos ASFF de nível superior, consultethe section called “Atributos opcionais de nível superior”.

```
"Findings": [
    {
     "Action": {
      "ActionType": "string",
      "AwsApiCallAction": {
       "AffectedResources": {
        "string": "string"
       },
       "Api": "string",
       "CallerType": "string",
       "DomainDetails": {
        "Domain": "string"
       },
```

```
        "FirstSeen": "string",
        "LastSeen": "string",
        "RemoteIpDetails": {
         "City": {
          "CityName": "string"
         },
         "Country": {
          "CountryCode": "string",
          "CountryName": "string"
         },
         "IpAddressV4": "string",
         "Geolocation": {
          "Lat": number,
          "Lon": number
         },
         "Organization": {
          "Asn": number,
          "AsnOrg": "string",
          "Isp": "string",
          "Org": "string"
         }
        },
        "ServiceName": "string"
       },
       "DnsRequestAction": {
        "Blocked": boolean,
        "Domain": "string",
        "Protocol": "string"
       },
       "NetworkConnectionAction": {
        "Blocked": boolean,
        "ConnectionDirection": "string",
        "LocalPortDetails": {
         "Port": number,
         "PortName": "string"
        },
        "Protocol": "string",
        "RemoteIpDetails": {
         "City": {
          "CityName": "string"
         },
         "Country": {
          "CountryCode": "string",
          "CountryName": "string"
```

```
        },
        "IpAddressV4": "string",
        "Geolocation": {
         "Lat": number,
         "Lon": number
        },
        "Organization": {
         "Asn": number,
         "AsnOrg": "string",
         "Isp": "string",
         "Org": "string"
        }
       },
       "RemotePortDetails": {
        "Port": number,
        "PortName": "string"
       }
      },
      "PortProbeAction": {
       "Blocked": boolean,
       "PortProbeDetails": [{
        "LocalIpDetails": {
         "IpAddressV4": "string"
        },
        "LocalPortDetails": {
         "Port": number,
         "PortName": "string"
        },
        "RemoteIpDetails": {
         "City": {
          "CityName": "string"
         },
         "Country": {
          "CountryCode": "string",
          "CountryName": "string"
         },
         "GeoLocation": {
          "Lat": number,
          "Lon": number
         },
         "IpAddressV4": "string",
         "Organization": {
          "Asn": number,
          "AsnOrg": "string",
```

```
          "Isp": "string",
          "Org": "string"
        }
       }
      }]
     }
    },
    "AwsAccountId": "string",
    "AwsAccountName": "string",
    "CompanyName": "string",
    "Compliance": {
     "AssociatedStandards": [{
      "StandardsId": "string"
     }],
     "RelatedRequirements": ["string"],
     "SecurityControlId": "string",
     "SecurityControlParameters": [
      {
       "Name": "string",
       "Value": ["string"]
      }
    ],
     "Status": "string",
     "StatusReasons": [
      {
       "Description": "string",
       "ReasonCode": "string"
      }
     ]
    },
    "Confidence": number,
    "CreatedAt": "string",
    "Criticality": number,
    "Description": "string",
    "FindingProviderFields": {
     "Confidence": number,
     "Criticality": number,
     "RelatedFindings": [{
      "ProductArn": "string",
      "Id": "string"
     }],
     "Severity": {
      "Label": "string",
      "Normalized": number,
```

```
        "Original": "string"
       },
       "Types": ["string"]
      },
      "FirstObservedAt": "string",
      "GeneratorId": "string",
      "Id": "string",
      "LastObservedAt": "string",
      "Malware": [{
       "Name": "string",
       "Path": "string",
       "State": "string",
       "Type": "string"
      }],
      "Network": {
       "DestinationDomain": "string",
       "DestinationIpV4": "string",
       "DestinationIpV6": "string",
       "DestinationPort": number,
       "Direction": "string",
       "OpenPortRange": {
        "Begin": integer,
        "End": integer
       },
       "Protocol": "string",
       "SourceDomain": "string",
       "SourceIpV4": "string",
       "SourceIpV6": "string",
       "SourceMac": "string",
       "SourcePort": number
      },
      "NetworkPath": [{
       "ComponentId": "string",
       "ComponentType": "string",
       "Egress": {
        "Destination": {
         "Address": ["string"],
         "PortRanges": [{
          "Begin": integer,
          "End": integer
         }]
        },
        "Protocol": "string",
        "Source": {
```

```
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       }
      },
      "Ingress": {
       "Destination": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       },
       "Protocol": "string",
       "Source": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       }
      }
     }],
     "Note": {
      "Text": "string",
      "UpdatedAt": "string",
      "UpdatedBy": "string"
     },
     "PatchSummary": {
      "FailedCount": number,
      "Id": "string",
      "InstalledCount": number,
      "InstalledOtherCount": number,
      "InstalledPendingReboot": number,
      "InstalledRejectedCount": number,
      "MissingCount": number,
      "Operation": "string",
      "OperationEndTime": "string",
      "OperationStartTime": "string",
      "RebootOption": "string"
     },
     "Process": {
```

```
      "LaunchedAt": "string",
      "Name": "string",
      "ParentPid": number,
      "Path": "string",
      "Pid": number,
      "TerminatedAt": "string"
     },
     "ProductArn": "string",
     "ProductFields": {
      "string": "string"
     },
     "ProductName": "string",
     "RecordState": "string",
     "Region": "string",
     "RelatedFindings": [{
      "Id": "string",
      "ProductArn": "string"
     }],
     "Remediation": {
      "Recommendation": {
       "Text": "string",
       "Url": "string"
      }
     },
     "Resources": [{
      "ApplicationArn": "string",
      "ApplicationName": "string",
      "DataClassification": {
       "DetailedResultsLocation": "string",
       "Result": {
        "AdditionalOccurrences": boolean,
        "CustomDataIdentifiers": {
         "Detections": [{
          "Arn": "string",
          "Count": integer,
          "Name": "string",
          "Occurrences": {
           "Cells": [{
            "CellReference": "string",
            "Column": integer,
            "ColumnName": "string",
            "Row": integer
           }],
           "LineRanges": [{
```

```
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "OffsetRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "Pages": [{
            "LineRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "OffsetRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
           }]
          }
         }],
         "TotalCount": integer
        },
        "MimeType": "string",
        "SensitiveData": [{
         "Category": "string",
         "Detections": [{
          "Count": integer,
          "Occurrences": {
           "Cells": [{
            "CellReference": "string",
            "Column": integer,
            "ColumnName": "string",
            "Row": integer
           }],
           "LineRanges": [{
            "End": integer,
```

```
            "Start": integer,
            "StartColumn": integer
           }],
           "OffsetRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           }],
           "Pages": [{
            "LineRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "OffsetRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
           }]
          },
          "Type": "string"
         }],
         "TotalCount": integer
        }],
        "SizeClassified": integer,
        "Status": {
         "Code": "string",
         "Reason": "string"
        }
       }
      },
      "Details": {
       "AwsAmazonMQBroker": {
        "AutoMinorVersionUpgrade": boolean,
        "BrokerArn": "string",
        "BrokerId": "string",
        "BrokerName": "string",
        "Configuration": {
```

```
          "Id": "string",
          "Revision": integer
         },
         "DeploymentMode": "string",
         "EncryptionOptions": {
          "UseAwsOwnedKey": boolean
         },
         "EngineType": "string",
         "EngineVersion": "string",
         "HostInstanceType": "string",
         "Logs": {
          "Audit": boolean,
          "AuditLogGroup": "string",
          "General": boolean,
          "GeneralLogGroup": "string"
         },
         "MaintenanceWindowStartTime": {
          "DayOfWeek": "string",
          "TimeOfDay": "string",
          "TimeZone": "string"
         },
         "PubliclyAccessible": boolean,
         "SecurityGroups": [
          "string"
         ],
         "StorageType": "string",
         "SubnetIds": [
          "string",
          "string"
         ],
         "Users": [{
          "Username": "string"
         }]
        },
        "AwsApiGatewayRestApi": {
         "ApiKeySource": "string",
         "BinaryMediaTypes": [" string"],
         "CreatedDate": "string",
         "Description": "string",
         "EndpointConfiguration": {
          "Types": ["string"]
         },
         "Id": "string",
         "MinimumCompressionSize": number,
```

```
        "Name": "string",
        "Version": "string"
       },
       "AwsApiGatewayStage": {
        "AccessLogSettings": {
         "DestinationArn": "string",
         "Format": "string"
        },
        "CacheClusterEnabled": boolean,
        "CacheClusterSize": "string",
        "CacheClusterStatus": "string",
        "CanarySettings": {
         "DeploymentId": "string",
         "PercentTraffic": number,
         "StageVariableOverrides": [{
          "string": "string"
         }],
         "UseStageCache": boolean
        },
        "ClientCertificateId": "string",
        "CreatedDate": "string",
        "DeploymentId": "string",
        "Description": "string",
        "DocumentationVersion": "string",
        "LastUpdatedDate": "string",
        "MethodSettings": [{
         "CacheDataEncrypted": boolean,
         "CachingEnabled": boolean,
         "CacheTtlInSeconds": number,
         "DataTraceEnabled": boolean,
         "HttpMethod": "string",
         "LoggingLevel": "string",
         "MetricsEnabled": boolean,
         "RequireAuthorizationForCacheControl": boolean,
         "ResourcePath": "string",
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number,
         "UnauthorizedCacheControlHeaderStrategy": "string"
        }],
        "StageName": "string",
        "TracingEnabled": boolean,
        "Variables": {
         "string": "string"
        },
```

```
        "WebAclArn": "string"
       },
       "AwsApiGatewayV2Api": {
        "ApiEndpoint": "string",
        "ApiId": "string",
        "ApiKeySelectionExpression": "string",
        "CorsConfiguration": {
         "AllowCredentials": boolean,
         "AllowHeaders": ["string"],
         "AllowMethods": ["string"],
         "AllowOrigins": ["string"],
         "ExposeHeaders": ["string"],
         "MaxAge": number
        },
        "CreatedDate": "string",
        "Description": "string",
        "Name": "string",
        "ProtocolType": "string",
        "RouteSelectionExpression": "string",
        "Version": "string"
       },
       "AwsApiGatewayV2Stage": {
        "AccessLogSettings": {
         "DestinationArn": "string",
         "Format": "string"
        },
        "ApiGatewayManaged": boolean,
        "AutoDeploy": boolean,
        "ClientCertificateId": "string",
        "CreatedDate": "string",
        "DefaultRouteSettings": {
         "DataTraceEnabled": boolean,
         "DetailedMetricsEnabled": boolean,
         "LoggingLevel": "string",
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number
        },
        "DeploymentId": "string",
        "Description": "string",
        "LastDeploymentStatusMessage": "string",
        "LastUpdatedDate": "string",
        "RouteSettings": {
         "DetailedMetricsEnabled": boolean,
         "LoggingLevel": "string",
```

```
          "DataTraceEnabled": boolean,
          "ThrottlingBurstLimit": number,
          "ThrottlingRateLimit": number
         },
         "StageName": "string",
         "StageVariables": [{
          "string": "string"
         }]
        },
        "AwsAppSyncGraphQLApi": {
         "AwsAppSyncGraphQlApi": {
          "AdditionalAuthenticationProviders": [
          {
           "AuthenticationType": "string",
           "LambdaAuthorizerConfig": {
            "AuthorizerResultTtlInSeconds": integer,
            "AuthorizerUri": "string"
           }
          },
          {
           "AuthenticationType": "string"
          }
          ],
          "ApiId": "string",
          "Arn": "string",
          "AuthenticationType": "string",
          "Id": "string",
          "LogConfig": {
           "CloudWatchLogsRoleArn": "string",
           "ExcludeVerboseContent": boolean,
           "FieldLogLevel": "string"
          },
          "Name": "string",
          "XrayEnabled": boolean
         }
        },
        "AwsAthenaWorkGroup": {
         "Description": "string",
         "Name": "string",
         "WorkgroupConfiguration": {
          "ResultConfiguration": {
           "EncryptionConfiguration": {
            "EncryptionOption": "string",
            "KmsKey": "string"
```

```
          }
         }
        },
        "State": "string"
       },
       "AwsAutoScalingAutoScalingGroup": {
        "AvailabilityZones": [{
         "Value": "string"
        }],
        "CreatedTime": "string",
        "HealthCheckGracePeriod": integer,
        "HealthCheckType": "string",
        "LaunchConfigurationName": "string",
        "LoadBalancerNames": ["string"],
        "LaunchTemplate": {
                       "LaunchTemplateId": "string",
                       "LaunchTemplateName": "string",
                       "Version": "string"
                   },
        "MixedInstancesPolicy": {
         "InstancesDistribution": {
          "OnDemandAllocationStrategy": "string",
          "OnDemandBaseCapacity": number,
          "OnDemandPercentageAboveBaseCapacity": number,
          "SpotAllocationStrategy": "string",
          "SpotInstancePools": number,
          "SpotMaxPrice": "string"
         },
         "LaunchTemplate": {
          "LaunchTemplateSpecification": {
           "LaunchTemplateId": "string",
           "LaunchTemplateName": "string",
           "Version": "string"
          },
          "CapacityRebalance": boolean,
          "Overrides": [{
           "InstanceType": "string",
           "WeightedCapacity": "string"
          }]
         }
        }
       },
       "AwsAutoScalingLaunchConfiguration": {
        "AssociatePublicIpAddress": boolean,
```

```
        "BlockDeviceMappings": [{
         "DeviceName": "string",
         "Ebs": {
          "DeleteOnTermination": boolean,
          "Encrypted": boolean,
          "Iops": number,
          "SnapshotId": "string",
          "VolumeSize": number,
          "VolumeType": "string"
         },
         "NoDevice": boolean,
         "VirtualName": "string"
        }],
        "ClassicLinkVpcId": "string",
        "ClassicLinkVpcSecurityGroups": ["string"],
        "CreatedTime": "string",
        "EbsOptimized": boolean,
        "IamInstanceProfile": "string"
       },
       "ImageId": "string",
       "InstanceMonitoring": {
        "Enabled": boolean
       },
       "InstanceType": "string",
       "KernelId": "string",
       "KeyName": "string",
       "LaunchConfigurationName": "string",
       "MetadataOptions": {
        "HttpEndPoint": "string",
        "HttpPutReponseHopLimit": number,
        "HttpTokens": "string"
       },
       "PlacementTenancy": "string",
       "RamdiskId": "string",
       "SecurityGroups": ["string"],
       "SpotPrice": "string",
       "UserData": "string"
      },
      "AwsBackupBackupPlan": {
       "BackupPlan": {
        "AdvancedBackupSettings": [{
         "BackupOptions": {
          "WindowsVSS":"string"
         },
```

```
          "ResourceType":"string"
        }],
        "BackupPlanName": "string",
        "BackupPlanRule": [{
         "CompletionWindowMinutes": integer,
         "CopyActions": [{
          "DestinationBackupVaultArn": "string",
          "Lifecycle": {
           "DeleteAfterDays": integer,
           "MoveToColdStorageAfterDays": integer
          }
         }],
         "Lifecycle": {
          "DeleteAfterDays": integer
         },
         "RuleName": "string",
         "ScheduleExpression": "string",
         "StartWindowMinutes": integer,
         "TargetBackupVault": "string"
        }]
       },
       "BackupPlanArn": "string",
       "BackupPlanId": "string",
       "VersionId": "string"
      },
      "AwsBackupBackupVault": {
       "AccessPolicy": {
        "Statement": [{
         "Action": ["string"],
         "Effect": "string",
         "Principal": {
          "AWS": "string"
         },
         "Resource": "string"
        }],
        "Version": "string"
       },
       "BackupVaultArn": "string",
       "BackupVaultName": "string",
       "EncryptionKeyArn": "string",
       "Notifications": {
        "BackupVaultEvents": ["string"],
        "SNSTopicArn": "string"
       }
```

```
      },
      "AwsBackupRecoveryPoint": {
       "BackupSizeInBytes": integer,
       "BackupVaultName": "string",
       "BackupVaultArn": "string",
       "CalculatedLifecycle": {
        "DeleteAt": "string",
        "MoveToColdStorageAt": "string"
       },
       "CompletionDate": "string",
       "CreatedBy": {
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
        "BackupPlanVersion": "string",
        "BackupRuleId": "string"
       },
       "CreationDate": "string",
       "EncryptionKeyArn": "string",
       "IamRoleArn": "string",
       "IsEncrypted": boolean,
       "LastRestoreTime": "string",
       "Lifecycle": {
        "DeleteAfterDays": integer,
        "MoveToColdStorageAfterDays": integer
       },
       "RecoveryPointArn": "string",
       "ResourceArn": "string",
       "ResourceType": "string",
       "SourceBackupVaultArn": "string",
       "Status": "string",
       "StatusMessage": "string",
       "StorageClass": "string"
      },
      "AwsCertificateManagerCertificate": {
       "CertificateAuthorityArn": "string",
       "CreatedAt": "string",
       "DomainName": "string",
       "DomainValidationOptions": [{
        "DomainName": "string",
        "ResourceRecord": {
         "Name": "string",
         "Type": "string",
         "Value": "string"
        },
```

```
        "ValidationDomain": "string",
        "ValidationEmails": ["string"],
        "ValidationMethod": "string",
        "ValidationStatus": "string"
      }],
      "ExtendedKeyUsages": [{
        "Name": "string",
        "OId": "string"
      }],
      "FailureReason": "string",
      "ImportedAt": "string",
      "InUseBy": ["string"],
      "IssuedAt": "string",
      "Issuer": "string",
      "KeyAlgorithm": "string",
      "KeyUsages": [{
        "Name": "string"
      }],
      "NotAfter": "string",
      "NotBefore": "string",
      "Options": {
        "CertificateTransparencyLoggingPreference": "string"
      },
      "RenewalEligibility": "string",
      "RenewalSummary": {
        "DomainValidationOptions": [{
          "DomainName": "string",
          "ResourceRecord": {
            "Name": "string",
            "Type": "string",
            "Value": "string"
          },
          "ValidationDomain": "string",
          "ValidationEmails": ["string"],
          "ValidationMethod": "string",
          "ValidationStatus": "string"
        }],
        "RenewalStatus": "string",
        "RenewalStatusReason": "string",
        "UpdatedAt": "string"
      },
      "Serial": "string",
      "SignatureAlgorithm": "string",
      "Status": "string",
```

```
        "Subject": "string",
        "SubjectAlternativeNames": ["string"],
        "Type": "string"
      },
      "AwsCloudFormationStack": {
        "Capabilities": ["string"],
        "CreationTime": "string",
        "Description": "string",
        "DisableRollback": boolean,
        "DriftInformation": {
          "StackDriftStatus": "string"
        },
        "EnableTerminationProtection": boolean,
        "LastUpdatedTime": "string",
        "NotificationArns": ["string"],
        "Outputs": [{
          "Description": "string",
          "OutputKey": "string",
          "OutputValue": "string"
        }],
        "RoleArn": "string",
        "StackId": "string",
        "StackName": "string",
        "StackStatus": "string",
        "StackStatusReason": "string",
        "TimeoutInMinutes": number
      },
      "AwsCloudFrontDistribution": {
        "CacheBehaviors": {
          "Items": [{
            "ViewerProtocolPolicy": "string"
          }]
        },
        "DefaultCacheBehavior": {
          "ViewerProtocolPolicy": "string"
        },
        "DefaultRootObject": "string",
        "DomainName": "string",
        "Etag": "string",
        "LastModifiedTime": "string",
        "Logging": {
          "Bucket": "string",
          "Enabled": boolean,
          "IncludeCookies": boolean,
```

```
        "Prefix": "string"
       },
       "OriginGroups": {
        "Items": [{
         "FailoverCriteria": {
          "StatusCodes": {
           "Items": [number],
           "Quantity": number
          }
         }
        }]
       },
       "Origins": {
        "Items": [{
         "CustomOriginConfig": {
          "HttpPort": number,
          "HttpsPort": number,
          "OriginKeepaliveTimeout": number,
          "OriginProtocolPolicy": "string",
          "OriginReadTimeout": number,
          "OriginSslProtocols": {
           "Items": ["string"],
           "Quantity": number
          }
         },
         "DomainName": "string",
         "Id": "string",
         "OriginPath": "string",
         "S3OriginConfig": {
          "OriginAccessIdentity": "string"
         }
        }]
       },
       "Status": "string",
       "ViewerCertificate": {
        "AcmCertificateArn": "string",
        "Certificate": "string",
        "CertificateSource": "string",
        "CloudFrontDefaultCertificate": boolean,
        "IamCertificateId": "string",
        "MinimumProtocolVersion": "string",
        "SslSupportMethod": "string"
       },
       "WebAclId": "string"
```

```
      },
      "AwsCloudTrailTrail": {
       "CloudWatchLogsLogGroupArn": "string",
       "CloudWatchLogsRoleArn": "string",
       "HasCustomEventSelectors": boolean,
       "HomeRegion": "string",
       "IncludeGlobalServiceEvents": boolean,
       "IsMultiRegionTrail": boolean,
       "IsOrganizationTrail": boolean,
       "KmsKeyId": "string",
       "LogFileValidationEnabled": boolean,
       "Name": "string",
       "S3BucketName": "string",
       "S3KeyPrefix": "string",
       "SnsTopicArn": "string",
       "SnsTopicName": "string",
       "TrailArn": "string"
      },
      "AwsCloudWatchAlarm": {
       "ActionsEnabled": boolean,
       "AlarmActions": ["string"],
       "AlarmArn": "string",
       "AlarmConfigurationUpdatedTimestamp": "string",
       "AlarmDescription": "string",
       "AlarmName": "string",
       "ComparisonOperator": "string",
       "DatapointsToAlarm": number,
       "Dimensions": [{
        "Name": "string",
        "Value": "string"
       }],
       "EvaluateLowSampleCountPercentile": "string",
       "EvaluationPeriods": number,
       "ExtendedStatistic": "string",
       "InsufficientDataActions": ["string"],
       "MetricName": "string",
       "Namespace": "string",
       "OkActions": ["string"],
       "Period": number,
       "Statistic": "string",
       "Threshold": number,
       "ThresholdMetricId": "string",
       "TreatMissingData": "string",
       "Unit": "string"
```

```
      },
      "AwsCodeBuildProject": {
       "Artifacts": [{
        "ArtifactIdentifier": "string",
        "EncryptionDisabled": boolean,
        "Location": "string",
        "Name": "string",
        "NamespaceType": "string",
        "OverrideArtifactName": boolean,
        "Packaging": "string",
        "Path": "string",
        "Type": "string"
       }],
       "SecondaryArtifacts": [{
                   "ArtifactIdentifier": "string",
                   "Type": "string",
                   "Location": "string",
                   "Name": "string",
                   "NamespaceType": "string",
                   "Packaging": "string",
                   "Path": "string",
                   "EncryptionDisabled": boolean,
                   "OverrideArtifactName": boolean
               }],
       "EncryptionKey": "string",
       "Certificate": "string",
       "Environment": {
        "Certificate": "string",
        "EnvironmentVariables": [{
         "Name": "string",
         "Type": "string",
         "Value": "string"
        }],
        "ImagePullCredentialsType": "string",
        "PrivilegedMode": boolean,
        "RegistryCredential": {
         "Credential": "string",
         "CredentialProvider": "string"
        },
        "Type": "string"
       },
       "LogsConfig": {
        "CloudWatchLogs": {
         "GroupName": "string",
```

```
          "Status": "string",
          "StreamName": "string"
         },
         "S3Logs": {
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Status": "string"
         }
        },
        "Name": "string",
        "ServiceRole": "string",
        "Source": {
         "Type": "string",
         "Location": "string",
         "GitCloneDepth": integer
        },
        "VpcConfig": {
         "VpcId": "string",
         "Subnets": ["string"],
         "SecurityGroupIds": ["string"]
        }
       },
       "AwsDmsEndpoint": {
        "CertificateArn": "string",
        "DatabaseName": "string",
        "EndpointArn": "string",
        "EndpointIdentifier": "string",
        "EndpointType": "string",
        "EngineName": "string",
        "KmsKeyId": "string",
        "Port": integer,
        "ServerName": "string",
        "SslMode": "string",
        "Username": "string"
       },
       "AwsDmsReplicationInstance": {
        "AllocatedStorage": integer,
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZone": "string",
        "EngineVersion": "string",
        "KmsKeyId": "string",
        "MultiAZ": boolean,
        "PreferredMaintenanceWindow": "string",
        "PubliclyAccessible": boolean,
```

```
        "ReplicationInstanceClass": "string",
        "ReplicationInstanceIdentifier": "string",
        "ReplicationSubnetGroup": {
            "ReplicationSubnetGroupIdentifier": "string"
        },
        "VpcSecurityGroups": [
            {
                "VpcSecurityGroupId": "string"
            }
        ]
      },
      "AwsDmsReplicationTask": {
        "CdcStartPosition": "string",
        "Id": "string",
        "MigrationType": "string",
        "ReplicationInstanceArn": "string",
        "ReplicationTaskIdentifier": "string",
        "ReplicationTaskSettings": {
          "string": "string"
        },
        "SourceEndpointArn": "string",
        "TableMappings": {
          "string": "string"
        },
        "TargetEndpointArn": "string"
      },
      "AwsDynamoDbTable": {
        "AttributeDefinitions": [{
          "AttributeName": "string",
          "AttributeType": "string"
        }],
        "BillingModeSummary": {
          "BillingMode": "string",
          "LastUpdateToPayPerRequestDateTime": "string"
        },
        "CreationDateTime": "string",
        "DeletionProtectionEnabled": boolean,
        "GlobalSecondaryIndexes": [{
          "Backfilling": boolean,
          "IndexArn": "string",
          "IndexName": "string",
          "IndexSizeBytes": number,
          "IndexStatus": "string",
          "ItemCount": number,
```

```
        "KeySchema": [{
         "AttributeName": "string",
         "KeyType": "string"
        }],
        "Projection": {
         "NonKeyAttributes": ["string"],
         "ProjectionType": "string"
        },
        "ProvisionedThroughput": {
         "LastDecreaseDateTime": "string",
         "LastIncreaseDateTime": "string",
         "NumberOfDecreasesToday": number,
         "ReadCapacityUnits": number,
         "WriteCapacityUnits": number
        }
       }],
       "GlobalTableVersion": "string",
       "ItemCount": number,
       "KeySchema": [{
        "AttributeName": "string",
        "KeyType": "string"
       }],
       "LatestStreamArn": "string",
       "LatestStreamLabel": "string",
       "LocalSecondaryIndexes": [{
        "IndexArn": "string",
        "IndexName": "string",
        "KeySchema": [{
         "AttributeName": "string",
         "KeyType": "string"
        }],
        "Projection": {
         "NonKeyAttributes": ["string"],
         "ProjectionType": "string"
        }
       }],
       "ProvisionedThroughput": {
        "LastDecreaseDateTime": "string",
        "LastIncreaseDateTime": "string",
        "NumberOfDecreasesToday": number,
        "ReadCapacityUnits": number,
        "WriteCapacityUnits": number
       },
       "Replicas": [{
```

```
        "GlobalSecondaryIndexes": [{
         "IndexName": "string",
         "ProvisionedThroughputOverride": {
          "ReadCapacityUnits": number
         }
        }],
        "KmsMasterKeyId": "string",
        "ProvisionedThroughputOverride": {
         "ReadCapacityUnits": number
        },
        "RegionName": "string",
        "ReplicaStatus": "string",
        "ReplicaStatusDescription": "string"
       }],
       "RestoreSummary": {
        "RestoreDateTime": "string",
        "RestoreInProgress": boolean,
        "SourceBackupArn": "string",
        "SourceTableArn": "string"
       },
       "SseDescription": {
        "InaccessibleEncryptionDateTime": "string",
        "KmsMasterKeyArn": "string",
        "SseType": "string",
        "Status": "string"
       },
       "StreamSpecification": {
        "StreamEnabled": boolean,
        "StreamViewType": "string"
       },
       "TableId": "string",
       "TableName": "string",
       "TableSizeBytes": number,
       "TableStatus": "string"
      },
      "AwsEc2ClientVpnEndpoint": {
       "AuthenticationOptions": [
        {
         "MutualAuthentication": {
          "ClientRootCertificateChainArn": "string"
         },
         "Type": "string"
        }
       ],
```

```
        "ClientCidrBlock": "string",
        "ClientConnectOptions": {
         "Enabled": boolean
        },
        "ClientLoginBannerOptions": {
         "Enabled": boolean
        },
        "ClientVpnEndpointId": "string",
        "ConnectionLogOptions": {
         "Enabled": boolean
        },
        "Description": "string",
        "DnsServer": ["string"],
        "ServerCertificateArn": "string",
        "SecurityGroupIdSet": [
         "string"
        ],
        "SelfServicePortalUrl": "string",
        "SessionTimeoutHours": "integer",
        "SplitTunnel": boolean,
        "TransportProtocol": "string",
        "VpcId": "string",
        "VpnPort": integer
       },
       "AwsEc2Eip": {
        "AllocationId": "string",
        "AssociationId": "string",
        "Domain": "string",
        "InstanceId": "string",
        "NetworkBorderGroup": "string",
        "NetworkInterfaceId": "string",
        "NetworkInterfaceOwnerId": "string",
        "PrivateIpAddress": "string",
        "PublicIp": "string",
        "PublicIpv4Pool": "string"
       },
       "AwsEc2Instance": {
        "IamInstanceProfileArn": "string",
        "ImageId": "string",
        "IpV4Addresses": ["string"],
        "IpV6Addresses": ["string"],
        "KeyName": "string",
        "LaunchedAt": "string",
        "MetadataOptions": {
```

```
        "HttpEndpoint": "string",
        "HttpProtocolIpv6": "string",
        "HttpPutResponseHopLimit": number,
        "HttpTokens": "string",
        "InstanceMetadataTags": "string"
       },
       "Monitoring": {
        "State": "string"
       },
       "NetworkInterfaces": [{
        "NetworkInterfaceId": "string"
       }],
       "SubnetId": "string",
       "Type": "string",
       "VirtualizationType": "string",
       "VpcId": "string"
      },
      "AwsEc2LaunchTemplate": {
       "DefaultVersionNumber": "string",
       "ElasticGpuSpecifications": ["string"],
       "ElasticInferenceAccelerators": ["string"],
       "Id": "string",
       "ImageId": "string",
       "LatestVersionNumber": "string",
       "LaunchTemplateData": {
        "BlockDeviceMappings": [{
         "DeviceName": "string",
         "Ebs": {
          "DeleteonTermination": boolean,
          "Encrypted": boolean,
          "SnapshotId": "string",
          "VolumeSize": number,
          "VolumeType": "string"
         }
        }],
        "MetadataOptions": {
         "HttpTokens": "string",
         "HttpPutResponseHopLimit" : number
        },
        "Monitoring": {
         "Enabled": boolean
        },
        "NetworkInterfaces": [{
         "AssociatePublicIpAddress" : boolean
```

```
        }]
       },
       "LaunchTemplateName": "string",
       "LicenseSpecifications": ["string"],
       "SecurityGroupIds": ["string"],
       "SecurityGroups": ["string"],
       "TagSpecifications": ["string"]
      },
      "AwsEc2NetworkAcl": {
       "Associations": [{
        "NetworkAclAssociationId": "string",
        "NetworkAclId": "string",
        "SubnetId": "string"
       }],
       "Entries": [{
        "CidrBlock": "string",
        "Egress": boolean,
        "IcmpTypeCode": {
         "Code": number,
         "Type": number
        },
        "Ipv6CidrBlock": "string",
        "PortRange": {
         "From": number,
         "To": number
        },
        "Protocol": "string",
        "RuleAction": "string",
        "RuleNumber": number
       }],
       "IsDefault": boolean,
       "NetworkAclId": "string",
       "OwnerId": "string",
       "VpcId": "string"
      },
      "AwsEc2NetworkInterface": {
       "Attachment": {
        "AttachmentId": "string",
        "AttachTime": "string",
        "DeleteOnTermination": boolean,
        "DeviceIndex": number,
        "InstanceId": "string",
        "InstanceOwnerId": "string",
        "Status": "string"
```

```
        },
        "Ipv6Addresses": [{
         "Ipv6Address": "string"
        }],
        "NetworkInterfaceId": "string",
        "PrivateIpAddresses": [{
         "PrivateDnsName": "string",
         "PrivateIpAddress": "string"
        }],
        "PublicDnsName": "string",
        "PublicIp": "string",
        "SecurityGroups": [{
         "GroupId": "string",
         "GroupName": "string"
        }],
        "SourceDestCheck": boolean
       },
       "AwsEc2RouteTable": {
        "AssociationSet": [{
         "AssociationState": {
          "State": "string"
         },
         "Main": boolean,
         "RouteTableAssociationId": "string",
         "RouteTableId": "string"
        }],
        "PropogatingVgwSet": [],
        "RouteTableId": "string",
        "RouteSet": [
         {
          "DestinationCidrBlock": "string",
          "GatewayId": "string",
          "Origin": "string",
          "State": "string"
         },
         {
          "DestinationCidrBlock": "string",
          "GatewayId": "string",
          "Origin": "string",
          "State": "string"
         }
        ],
        "VpcId": "string"
       },
```

```
      "AwsEc2SecurityGroup": {
       "GroupId": "string",
       "GroupName": "string",
       "IpPermissions": [{
        "FromPort": number,
        "IpProtocol": "string",
        "IpRanges": [{
         "CidrIp": "string"
        }],
        "Ipv6Ranges": [{
         "CidrIpv6": "string"
        }],
        "PrefixListIds": [{
         "PrefixListId": "string"
        }],
        "ToPort": number,
        "UserIdGroupPairs": [{
         "GroupId": "string",
         "GroupName": "string",
         "PeeringStatus": "string",
         "UserId": "string",
         "VpcId": "string",
         "VpcPeeringConnectionId": "string"
        }]
       }],
       "IpPermissionsEgress": [{
        "FromPort": number,
        "IpProtocol": "string",
        "IpRanges": [{
         "CidrIp": "string"
        }],
        "Ipv6Ranges": [{
         "CidrIpv6": "string"
        }],
        "PrefixListIds": [{
         "PrefixListId": "string"
        }],
        "ToPort": number,
        "UserIdGroupPairs": [{
         "GroupId": "string",
         "GroupName": "string",
         "PeeringStatus": "string",
         "UserId": "string",
         "VpcId": "string",
```

```
          "VpcPeeringConnectionId": "string"
         }]
        }],
        "OwnerId": "string",
        "VpcId": "string"
       },
       "AwsEc2Subnet": {
        "AssignIpv6AddressOnCreation": boolean,
        "AvailabilityZone": "string",
        "AvailabilityZoneId": "string",
        "AvailableIpAddressCount": number,
        "CidrBlock": "string",
        "DefaultForAz": boolean,
        "Ipv6CidrBlockAssociationSet": [{
         "AssociationId": "string",
         "Ipv6CidrBlock": "string",
         "CidrBlockState": "string"
        }],
        "MapPublicIpOnLaunch": boolean,
        "OwnerId": "string",
        "State": "string",
        "SubnetArn": "string",
        "SubnetId": "string",
        "VpcId": "string"
       },
       "AwsEc2TransitGateway": {
        "AmazonSideAsn": number,
        "AssociationDefaultRouteTableId": "string",
        "AutoAcceptSharedAttachments": "string",
        "DefaultRouteTableAssociation": "string",
        "DefaultRouteTablePropagation": "string",
        "Description": "string",
        "DnsSupport": "string",
        "Id": "string",
        "MulticastSupport": "string",
        "PropagationDefaultRouteTableId": "string",
        "TransitGatewayCidrBlocks": ["string"],
        "VpnEcmpSupport": "string"
       },
       "AwsEc2Volume": {
        "Attachments": [{
         "AttachTime": "string",
         "DeleteOnTermination": boolean,
         "InstanceId": "string",
```

```
        "Status": "string"
       }],
       "CreateTime": "string",
       "DeviceName": "string",
       "Encrypted": boolean,
       "KmsKeyId": "string",
       "Size": number,
       "SnapshotId": "string",
       "Status": "string",
       "VolumeId": "string",
       "VolumeScanStatus": "string",
       "VolumeType": "string"
      },
      "AwsEc2Vpc": {
       "CidrBlockAssociationSet": [{
        "AssociationId": "string",
        "CidrBlock": "string",
        "CidrBlockState": "string"
       }],
       "DhcpOptionsId": "string",
       "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "string",
        "CidrBlockState": "string",
        "Ipv6CidrBlock": "string"
       }],
       "State": "string"
      },
      "AwsEc2VpcEndpointService": {
       "AcceptanceRequired": boolean,
       "AvailabilityZones": ["string"],
       "BaseEndpointDnsNames": ["string"],
       "ManagesVpcEndpoints": boolean,
       "GatewayLoadBalancerArns": ["string"],
       "NetworkLoadBalancerArns": ["string"],
       "PrivateDnsName": "string",
       "ServiceId": "string",
       "ServiceName": "string",
       "ServiceState": "string",
       "ServiceType": [{
        "ServiceType": "string"
       }]
      },
      "AwsEc2VpcPeeringConnection": {
       "AccepterVpcInfo": {
```

```
        "CidrBlock": "string",
        "CidrBlockSet": [{
         "CidrBlock": "string"
        }],
        "Ipv6CidrBlockSet": [{
         "Ipv6CidrBlock": "string"
        }],
        "OwnerId": "string",
        "PeeringOptions": {
         "AllowDnsResolutionFromRemoteVpc": boolean,
         "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
         "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
        },
        "Region": "string",
        "VpcId": "string"
       },
       "ExpirationTime": "string",
       "RequesterVpcInfo": {
        "CidrBlock": "string",
        "CidrBlockSet": [{
         "CidrBlock": "string"
        }],
        "Ipv6CidrBlockSet": [{
         "Ipv6CidrBlock": "string"
        }],
        "OwnerId": "string",
        "PeeringOptions": {
         "AllowDnsResolutionFromRemoteVpc": boolean,
         "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
         "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
        },
        "Region": "string",
        "VpcId": "string"
       },
       "Status": {
        "Code": "string",
        "Message": "string"
       },
       "VpcPeeringConnectionId": "string"
      },
      "AwsEc2VpnConnection": {
       "Category": "string",
       "CustomerGatewayConfiguration": "string",
       "CustomerGatewayId": "string",
```

```
        "Options": {
         "StaticRoutesOnly": boolean,
         "TunnelOptions": [{
          "DpdTimeoutSeconds": number,
          "IkeVersions": ["string"],
          "OutsideIpAddress": "string",
          "Phase1DhGroupNumbers": [number],
          "Phase1EncryptionAlgorithms": ["string"],
          "Phase1IntegrityAlgorithms": ["string"],
          "Phase1LifetimeSeconds": number,
          "Phase2DhGroupNumbers": [number],
          "Phase2EncryptionAlgorithms": ["string"],
          "Phase2IntegrityAlgorithms": ["string"],
          "Phase2LifetimeSeconds": number,
          "PreSharedKey": "string",
          "RekeyFuzzPercentage": number,
          "RekeyMarginTimeSeconds": number,
          "ReplayWindowSize": number,
          "TunnelInsideCidr": "string"
         }]
        },
        "Routes": [{
         "DestinationCidrBlock": "string",
         "State": "string"
        }],
        "State": "string",
        "TransitGatewayId": "string",
        "Type": "string",
        "VgwTelemetry": [{
         "AcceptedRouteCount": number,
         "CertificateArn": "string",
         "LastStatusChange": "string",
         "OutsideIpAddress": "string",
         "Status": "string",
         "StatusMessage": "string"
        }],
        "VpnConnectionId": "string",
        "VpnGatewayId": "string"
       },
       "AwsEcrContainerImage": {
        "Architecture": "string",
        "ImageDigest": "string",
        "ImagePublishedAt": "string",
        "ImageTags": ["string"],
```

```
        "RegistryId": "string",
        "RepositoryName": "string"
      },
      "AwsEcrRepository": {
        "Arn": "string",
        "ImageScanningConfiguration": {
          "ScanOnPush": boolean
        },
        "ImageTagMutability": "string",
        "LifecyclePolicy": {
          "LifecyclePolicyText": "string",
          "RegistryId": "string"
        },
        "RepositoryName": "string",
        "RepositoryPolicyText": "string"
      },
      "AwsEcsCluster": {
        "ActiveServicesCount": number,
        "CapacityProviders": ["string"],
        "ClusterArn": "string",
        "ClusterName": "string",
        "ClusterSettings": [{
          "Name": "string",
          "Value": "string"
        }],
        "Configuration": {
          "ExecuteCommandConfiguration": {
            "KmsKeyId": "string",
            "LogConfiguration": {
              "CloudWatchEncryptionEnabled": boolean,
              "CloudWatchLogGroupName": "string",
              "S3BucketName": "string",
              "S3EncryptionEnabled": boolean,
              "S3KeyPrefix": "string"
            },
            "Logging": "string"
          }
        },
        "DefaultCapacityProviderStrategy": [{
          "Base": number,
          "CapacityProvider": "string",
          "Weight": number
        }],
        "RegisteredContainerInstancesCount": number,
```

```
        "RunningTasksCount": number,
        "Status": "string"
      },
      "AwsEcsContainer": {
        "Image": "string",
        "MountPoints": [{
          "ContainerPath": "string",
          "SourceVolume": "string"
        }],
        "Name": "string",
        "Privileged": boolean
      },
      "AwsEcsService": {
        "CapacityProviderStrategy": [{
          "Base": number,
          "CapacityProvider": "string",
          "Weight": number
        }],
        "Cluster": "string",
        "DeploymentConfiguration": {
          "DeploymentCircuitBreaker": {
            "Enable": boolean,
            "Rollback": boolean
          },
          "MaximumPercent": number,
          "MinimumHealthyPercent": number
        },
        "DeploymentController": {
          "Type": "string"
        },
        "DesiredCount": number,
        "EnableEcsManagedTags": boolean,
        "EnableExecuteCommand": boolean,
        "HealthCheckGracePeriodSeconds": number,
        "LaunchType": "string",
        "LoadBalancers": [{
          "ContainerName": "string",
          "ContainerPort": number,
          "LoadBalancerName": "string",
          "TargetGroupArn": "string"
        }],
        "Name": "string",
        "NetworkConfiguration": {
          "AwsVpcConfiguration": {
```

```
          "AssignPublicIp": "string",
          "SecurityGroups": ["string"],
          "Subnets": ["string"]
         }
        },
        "PlacementConstraints": [{
         "Expression": "string",
         "Type": "string"
        }],
        "PlacementStrategies": [{
         "Field": "string",
         "Type": "string"
        }],
        "PlatformVersion": "string",
        "PropagateTags": "string",
        "Role": "string",
        "SchedulingStrategy": "string",
        "ServiceArn": "string",
        "ServiceName": "string",
        "ServiceRegistries": [{
         "ContainerName": "string",
         "ContainerPort": number,
         "Port": number,
         "RegistryArn": "string"
        }],
        "TaskDefinition": "string"
       },
       "AwsEcsTask": {
        "CreatedAt": "string",
        "ClusterArn": "string",
        "Group": "string",
        "StartedAt": "string",
        "StartedBy": "string",
        "TaskDefinitionArn": "string",
        "Version": number,
        "Volumes": [{
         "Name": "string",
         "Host": {
          "SourcePath": "string"
         }
        }],
        "Containers": [{
         "Image": "string",
         "MountPoints": [{
```

```
          "ContainerPath": "string",
          "SourceVolume": "string"
         }],
         "Name": "string",
         "Privileged": boolean
        }]
       },
       "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [{
         "Command": ["string"],
         "Cpu": number,
         "DependsOn": [{
          "Condition": "string",
          "ContainerName": "string"
         }],
         "DisableNetworking": boolean,
         "DnsSearchDomains": ["string"],
         "DnsServers": ["string"],
         "DockerLabels": {
          "string": "string"
         },
         "DockerSecurityOptions": ["string"],
         "EntryPoint": ["string"],
         "Environment": [{
          "Name": "string",
          "Value": "string"
         }],
         "EnvironmentFiles": [{
          "Type": "string",
          "Value": "string"
         }],
         "Essential": boolean,
         "ExtraHosts": [{
          "Hostname": "string",
          "IpAddress": "string"
         }],
         "FirelensConfiguration": {
          "Options": {
           "string": "string"
          },
          "Type": "string"
         },
         "HealthCheck": {
          "Command": ["string"],
```

```
          "Interval": number,
          "Retries": number,
          "StartPeriod": number,
          "Timeout": number
         },
         "Hostname": "string",
         "Image": "string",
         "Interactive": boolean,
         "Links": ["string"],
         "LinuxParameters": {
          "Capabilities": {
           "Add": ["string"],
           "Drop": ["string"]
          },
          "Devices": [{
           "ContainerPath": "string",
           "HostPath": "string",
           "Permissions": ["string"]
          }],
          "InitProcessEnabled": boolean,
          "MaxSwap": number,
          "SharedMemorySize": number,
          "Swappiness": number,
          "Tmpfs": [{
           "ContainerPath": "string",
           "MountOptions": ["string"],
           "Size": number
          }]
         },
         "LogConfiguration": {
          "LogDriver": "string",
          "Options": {
           "string": "string"
          },
          "SecretOptions": [{
           "Name": "string",
           "ValueFrom": "string"
          }]
         },
         "Memory": number,
         "MemoryReservation": number,
         "MountPoints": [{
          "ContainerPath": "string",
          "ReadOnly": boolean,
```

```
          "SourceVolume": "string"
         }],
         "Name": "string",
         "PortMappings": [{
          "ContainerPort": number,
          "HostPort": number,
          "Protocol": "string"
         }],
         "Privileged": boolean,
         "PseudoTerminal": boolean,
         "ReadonlyRootFilesystem": boolean,
         "RepositoryCredentials": {
          "CredentialsParameter": "string"
         },
         "ResourceRequirements": [{
          "Type": "string",
          "Value": "string"
         }],
         "Secrets": [{
          "Name": "string",
          "ValueFrom": "string"
         }],
         "StartTimeout": number,
         "StopTimeout": number,
         "SystemControls": [{
          "Namespace": "string",
          "Value": "string"
         }],
         "Ulimits": [{
          "HardLimit": number,
          "Name": "string",
          "SoftLimit": number
         }],
         "User": "string",
         "VolumesFrom": [{
          "ReadOnly": boolean,
          "SourceContainer": "string"
         }],
         "WorkingDirectory": "string"
        }],
        "Cpu": "string",
        "ExecutionRoleArn": "string",
        "Family": "string",
        "InferenceAccelerators": [{
```

```
        "DeviceName": "string",
        "DeviceType": "string"
       }],
       "IpcMode": "string",
       "Memory": "string",
       "NetworkMode": "string",
       "PidMode": "string",
       "PlacementConstraints": [{
        "Expression": "string",
        "Type": "string"
       }],
       "ProxyConfiguration": {
        "ContainerName": "string",
        "ProxyConfigurationProperties": [{
         "Name": "string",
         "Value": "string"
        }],
        "Type": "string"
       },
       "RequiresCompatibilities": ["string"],
       "Status": "string",
       "TaskRoleArn": "string",
       "Volumes": [{
        "DockerVolumeConfiguration": {
         "Autoprovision": boolean,
         "Driver": "string",
         "DriverOpts": {
          "string": "string"
         },
         "Labels": {
          "string": "string"
         },
         "Scope": "string"
        },
        "EfsVolumeConfiguration": {
         "AuthorizationConfig": {
          "AccessPointId": "string",
          "Iam": "string"
         },
         "FilesystemId": "string",
         "RootDirectory": "string",
         "TransitEncryption": "string",
         "TransitEncryptionPort": number
        },
```

```
        "Host": {
         "SourcePath": "string"
        },
        "Name": "string"
       }]
      },
      "AwsEfsAccessPoint": {
       "AccessPointId": "string",
       "Arn": "string",
       "ClientToken": "string",
       "FileSystemId": "string",
       "PosixUser": {
        "Gid": "string",
        "SecondaryGids": ["string"],
        "Uid": "string"
       },
       "RootDirectory": {
        "CreationInfo": {
         "OwnerGid": "string",
         "OwnerUid": "string",
         "Permissions": "string"
        },
        "Path": "string"
       }
      },
      "AwsEksCluster": {
       "Arn": "string",
       "CertificateAuthorityData": "string",
       "ClusterStatus": "string",
       "Endpoint": "string",
       "Logging": {
        "ClusterLogging": [{
         "Enabled": boolean,
         "Types": ["string"]
        }]
       },
       "Name": "string",
       "ResourcesVpcConfig": {
        "EndpointPublicAccess": boolean,
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
       },
       "RoleArn": "string",
       "Version": "string"
```

```
      },
      "AwsElasticBeanstalkEnvironment": {
       "ApplicationName": "string",
       "Cname": "string",
       "DateCreated": "string",
       "DateUpdated": "string",
       "Description": "string",
       "EndpointUrl": "string",
       "EnvironmentArn": "string",
       "EnvironmentId": "string",
       "EnvironmentLinks": [{
        "EnvironmentName": "string",
        "LinkName": "string"
       }],
       "EnvironmentName": "string",
       "OptionSettings": [{
        "Namespace": "string",
        "OptionName": "string",
        "ResourceName": "string",
        "Value": "string"
       }],
       "PlatformArn": "string",
       "SolutionStackName": "string",
       "Status": "string",
       "Tier": {
        "Name": "string",
        "Type": "string",
        "Version": "string"
       },
       "VersionLabel": "string"
      },
      "AwsElasticSearchDomain": {
       "AccessPolicies": "string",
       "DomainStatus": {
        "DomainId": "string",
        "DomainName": "string",
        "Endpoint": "string",
        "Endpoints": {
         "string": "string"
        }
       },
       "DomainEndpointOptions": {
        "EnforceHTTPS": boolean,
        "TLSSecurityPolicy": "string"
```

```
        },
        "ElasticsearchClusterConfig": {
         "DedicatedMasterCount": number,
         "DedicatedMasterEnabled": boolean,
         "DedicatedMasterType": "string",
         "InstanceCount": number,
         "InstanceType": "string",
         "ZoneAwarenessConfig": {
          "AvailabilityZoneCount": number
         },
         "ZoneAwarenessEnabled": boolean
        },
        "ElasticsearchVersion": "string",
        "EncryptionAtRestOptions": {
         "Enabled": boolean,
         "KmsKeyId": "string"
        },
        "LogPublishingOptions": {
         "AuditLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "IndexSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "SearchSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         }
        },
        "NodeToNodeEncryptionOptions": {
         "Enabled": boolean
        },
        "ServiceSoftwareOptions": {
         "AutomatedUpdateDate": "string",
         "Cancellable": boolean,
         "CurrentVersion": "string",
         "Description": "string",
         "NewVersion": "string",
         "UpdateAvailable": boolean,
         "UpdateStatus": "string"
        },
        "VPCOptions": {
```

```
        "AvailabilityZones": [
         "string"
        ],
        "SecurityGroupIds": [
         "string"
        ],
        "SubnetIds": [
         "string"
        ],
        "VPCId": "string"
       }
      },
      "AwsElbLoadBalancer": {
       "AvailabilityZones": ["string"],
       "BackendServerDescriptions": [{
        "InstancePort": number,
        "PolicyNames": ["string"]
       }],
       "CanonicalHostedZoneName": "string",
       "CanonicalHostedZoneNameID": "string",
       "CreatedTime": "string",
       "DnsName": "string",
       "HealthCheck": {
        "HealthyThreshold": number,
        "Interval": number,
        "Target": "string",
        "Timeout": number,
        "UnhealthyThreshold": number
       },
       "Instances": [{
        "InstanceId": "string"
       }],
       "ListenerDescriptions": [{
        "Listener": {
         "InstancePort": number,
         "InstanceProtocol": "string",
         "LoadBalancerPort": number,
         "Protocol": "string",
         "SslCertificateId": "string"
        },
        "PolicyNames": ["string"]
       }],
       "LoadBalancerAttributes": {
        "AccessLog": {
```

```
          "EmitInterval": number,
          "Enabled": boolean,
          "S3BucketName": "string",
          "S3BucketPrefix": "string"
         },
         "ConnectionDraining": {
          "Enabled": boolean,
          "Timeout": number
         },
         "ConnectionSettings": {
          "IdleTimeout": number
         },
         "CrossZoneLoadBalancing": {
          "Enabled": boolean
         },
         "AdditionalAttributes": [{
                        "Key": "string",
                        "Value": "string"
                    }]
        },
        "LoadBalancerName": "string",
        "Policies": {
         "AppCookieStickinessPolicies": [{
          "CookieName": "string",
          "PolicyName": "string"
         }],
         "LbCookieStickinessPolicies": [{
          "CookieExpirationPeriod": number,
          "PolicyName": "string"
         }],
         "OtherPolicies": ["string"]
        },
        "Scheme": "string",
        "SecurityGroups": ["string"],
        "SourceSecurityGroup": {
         "GroupName": "string",
         "OwnerAlias": "string"
        },
        "Subnets": ["string"],
        "VpcId": "string"
       },
       "AwsElbv2LoadBalancer": {
        "AvailabilityZones": {
         "SubnetId": "string",
```

```
        "ZoneName": "string"
       },
       "CanonicalHostedZoneId": "string",
       "CreatedTime": "string",
       "DNSName": "string",
       "IpAddressType": "string",
       "LoadBalancerAttributes": [{
        "Key": "string",
        "Value": "string"
       }],
       "Scheme": "string",
       "SecurityGroups": ["string"],
       "State": {
        "Code": "string",
        "Reason": "string"
       },
       "Type": "string",
       "VpcId": "string"
      },
      "AwsEventSchemasRegistry": {
       "Description": "string",
       "RegistryArn": "string",
       "RegistryName": "string"
      },
      "AwsEventsEndpoint": {
       "Arn": "string",
       "Description": "string",
       "EndpointId": "string",
       "EndpointUrl": "string",
       "EventBuses": [
           {
               "EventBusArn": "string"
           },
           {
               "EventBusArn": "string"
           }
       ],
       "Name": "string",
       "ReplicationConfig": {
           "State": "string"
       },
       "RoleArn": "string",
       "RoutingConfig": {
           "FailoverConfig": {
```

```
            "Primary": {
                "HealthCheck": "string"
            },
            "Secondary": {
                "Route": "string"
            }
        }
    },
    "State": "string"
  },
  "AwsEventsEventBus": {
    "Arn": "string",
    "Name": "string",
    "Policy": "string"
  },
  "AwsGuardDutyDetector": {
    "FindingPublishingFrequency": "string",
    "ServiceRole": "string",
    "Status": "string",
    "DataSources": {
      "CloudTrail": {
        "Status": "string"
      },
      "DnsLogs": {
        "Status": "string"
      },
      "FlowLogs": {
        "Status": "string"
      },
      "S3Logs": {
        "Status": "string"
      },
      "Kubernetes": {
        "AuditLogs": {
          "Status": "string"
        }
      },
      "MalwareProtection": {
        "ScanEc2InstanceWithFindings": {
          "EbsVolumes": {
            "Status": "string"
          }
        },
        "ServiceRole": "string"
```

```
        }
       }
      },
      "AwsIamAccessKey": {
       "AccessKeyId": "string",
       "AccountId": "string",
       "CreatedAt": "string",
       "PrincipalId": "string",
       "PrincipalName": "string",
       "PrincipalType": "string",
       "SessionContext": {
        "Attributes": {
         "CreationDate": "string",
         "MfaAuthenticated": boolean
        },
        "SessionIssuer": {
         "AccountId": "string",
         "Arn": "string",
         "PrincipalId": "string",
         "Type": "string",
         "UserName": "string"
        }
       },
       "Status": "string"
      },
      "AwsIamGroup": {
       "AttachedManagedPolicies": [{
        "PolicyArn": "string",
        "PolicyName": "string"
       }],
       "CreateDate": "string",
       "GroupId": "string",
       "GroupName": "string",
       "GroupPolicyList": [{
        "PolicyName": "string"
       }],
       "Path": "string"
      },
      "AwsIamPolicy": {
       "AttachmentCount": number,
       "CreateDate": "string",
       "DefaultVersionId": "string",
       "Description": "string",
       "IsAttachable": boolean,
```

```
        "Path": "string",
        "PermissionsBoundaryUsageCount": number,
        "PolicyId": "string",
        "PolicyName": "string",
        "PolicyVersionList": [{
         "CreateDate": "string",
         "IsDefaultVersion": boolean,
         "VersionId": "string"
        }],
        "UpdateDate": "string"
       },
       "AwsIamRole": {
        "AssumeRolePolicyDocument": "string",
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "InstanceProfileList": [{
         "Arn": "string",
         "CreateDate": "string",
         "InstanceProfileId": "string",
         "InstanceProfileName": "string",
         "Path": "string",
         "Roles": [{
          "Arn": "string",
          "AssumeRolePolicyDocument": "string",
          "CreateDate": "string",
          "Path": "string",
          "RoleId": "string",
          "RoleName": "string"
         }]
        }],
        "MaxSessionDuration": number,
        "Path": "string",
        "PermissionsBoundary": {
         "PermissionsBoundaryArn": "string",
         "PermissionsBoundaryType": "string"
        },
        "RoleId": "string",
        "RoleName": "string",
        "RolePolicyList": [{
         "PolicyName": "string"
        }]
```

```
      },
      "AwsIamUser": {
       "AttachedManagedPolicies": [{
        "PolicyArn": "string",
        "PolicyName": "string"
       }],
       "CreateDate": "string",
       "GroupList": ["string"],
       "Path": "string",
       "PermissionsBoundary": {
        "PermissionsBoundaryArn": "string",
        "PermissionsBoundaryType": "string"
       },
       "UserId": "string",
       "UserName": "string",
       "UserPolicyList": [{
        "PolicyName": "string"
       }]
      },
      "AwsKinesisStream": {
       "Arn": "string",
       "Name": "string",
       "RetentionPeriodHours": number,
       "ShardCount": number,
       "StreamEncryption": {
        "EncryptionType": "string",
        "KeyId": "string"
       }
      },
      "AwsKmsKey": {
       "AWSAccountId": "string",
       "CreationDate": "string",
       "Description": "string",
       "KeyId": "string",
       "KeyManager": "string",
       "KeyRotationStatus": boolean,
       "KeyState": "string",
       "Origin": "string"
      },
      "AwsLambdaFunction": {
       "Architectures": [
        "string"
       ],
       "Code": {
```

```
        "S3Bucket": "string",
        "S3Key": "string",
        "S3ObjectVersion": "string",
        "ZipFile": "string"
       },
       "CodeSha256": "string",
       "DeadLetterConfig": {
        "TargetArn": "string"
       },
       "Environment": {
        "Variables": {
         "Stage": "string"
        },
        "Error": {
         "ErrorCode": "string",
         "Message": "string"
        }
       },
       "FunctionName": "string",
       "Handler": "string",
       "KmsKeyArn": "string",
       "LastModified": "string",
       "Layers": {
        "Arn": "string",
        "CodeSize": number
       },
       "PackageType": "string",
       "RevisionId": "string",
       "Role": "string",
       "Runtime": "string",
       "Timeout": integer,
       "TracingConfig": {
        "Mode": "string"
       },
       "Version": "string",
       "VpcConfig": {
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
       },
       "MasterArn": "string",
       "MemorySize": number
      },
      "AwsLambdaLayerVersion": {
       "CompatibleRuntimes": [
```

```
        "string"
       ],
       "CreatedDate": "string",
       "Version": number
      },
      "AwsMskCluster": {
       "ClusterInfo": {
        "ClientAuthentication": {
         "Sasl": {
          "Scram": {
           "Enabled": boolean
          },
          "Iam": {
           "Enabled": boolean
          }
         },
         "Tls": {
          "CertificateAuthorityArnList": [],
          "Enabled": boolean
         },
         "Unauthenticated": {
          "Enabled": boolean
         }
        },
        "ClusterName": "string",
        "CurrentVersion": "string",
        "EncryptionInfo": {
         "EncryptionAtRest": {
          "DataVolumeKMSKeyId": "string"
         },
         "EncryptionInTransit": {
          "ClientBroker": "string",
          "InCluster": boolean
         }
        },
        "EnhancedMonitoring": "string",
        "NumberOfBrokerNodes": integer
       }
      },
      "AwsNetworkFirewallFirewall": {
       "DeleteProtection": boolean,
       "Description": "string",
       "FirewallArn": "string",
       "FirewallId": "string",
```

```
        "FirewallName": "string",
        "FirewallPolicyArn": "string",
        "FirewallPolicyChangeProtection": boolean,
        "SubnetChangeProtection": boolean,
        "SubnetMappings": [{
         "SubnetId": "string"
        }],
        "VpcId": "string"
       },
       "AwsNetworkFirewallFirewallPolicy": {
        "Description": "string",
        "FirewallPolicy": {
         "StatefulRuleGroupReferences": [{
          "ResourceArn": "string"
         }],
         "StatelessCustomActions": [{
          "ActionDefinition": {
           "PublishMetricAction": {
            "Dimensions": [{
             "Value": "string"
            }]
           }
          },
          "ActionName": "string"
         }],
         "StatelessDefaultActions": ["string"],
         "StatelessFragmentDefaultActions": ["string"],
         "StatelessRuleGroupReferences": [{
          "Priority": number,
          "ResourceArn": "string"
         }]
        },
        "FirewallPolicyArn": "string",
        "FirewallPolicyId": "string",
        "FirewallPolicyName": "string"
       },
       "AwsNetworkFirewallRuleGroup": {
        "Capacity": number,
        "Description": "string",
        "RuleGroup": {
         "RulesSource": {
          "RulesSourceList": {
           "GeneratedRulesType": "string",
           "Targets": ["string"],
```

```
          "TargetTypes": ["string"]
         },
         "RulesString": "string",
         "StatefulRules": [{
          "Action": "string",
          "Header": {
           "Destination": "string",
           "DestinationPort": "string",
           "Direction": "string",
           "Protocol": "string",
           "Source": "string",
           "SourcePort": "string"
          },
          "RuleOptions": [{
           "Keyword": "string",
           "Settings": ["string"]
          }]
         }],
         "StatelessRulesAndCustomActions": {
          "CustomActions": [{
           "ActionDefinition": {
            "PublishMetricAction": {
             "Dimensions": [{
              "Value": "string"
             }]
            }
           },
           "ActionName": "string"
          }],
          "StatelessRules": [{
           "Priority": number,
           "RuleDefinition": {
            "Actions": ["string"],
            "MatchAttributes": {
             "DestinationPorts": [{
              "FromPort": number,
              "ToPort": number
             }],
             "Destinations": [{
              "AddressDefinition": "string"
             }],
             "Protocols": [number],
             "SourcePorts": [{
              "FromPort": number,
```

```
            "ToPort": number
           }],
           "Sources": [{
            "AddressDefinition": "string"
           }],
           "TcpFlags": [{
            "Flags": ["string"],
            "Masks": ["string"]
           }]
          }
         }
        }]
       }
      },
      "RuleVariables": {
       "IpSets": {
        "Definition": ["string"]
       },
       "PortSets": {
        "Definition": ["string"]
       }
      }
     },
     "RuleGroupArn": "string",
     "RuleGroupId": "string",
     "RuleGroupName": "string",
     "Type": "string"
    },
    "AwsOpenSearchServiceDomain": {
     "AccessPolicies": "string",
     "AdvancedSecurityOptions": {
      "Enabled": boolean,
      "InternalUserDatabaseEnabled": boolean,
      "MasterUserOptions": {
       "MasterUserArn": "string",
       "MasterUserName": "string",
       "MasterUserPassword": "string"
      }
     },
     "Arn": "string",
     "ClusterConfig": {
      "DedicatedMasterCount": number,
      "DedicatedMasterEnabled": boolean,
      "DedicatedMasterType": "string",
```

```
        "InstanceCount": number,
        "InstanceType": "string",
        "WarmCount": number,
        "WarmEnabled": boolean,
        "WarmType": "string",
        "ZoneAwarenessConfig": {
          "AvailabilityZoneCount": number
        },
        "ZoneAwarenessEnabled": boolean
      },
      "DomainEndpoint": "string",
      "DomainEndpointOptions": {
        "CustomEndpoint": "string",
        "CustomEndpointCertificateArn": "string",
        "CustomEndpointEnabled": boolean,
        "EnforceHTTPS": boolean,
        "TLSSecurityPolicy": "string"
      },
      "DomainEndpoints": {
        "string": "string"
      },
      "DomainName": "string",
      "EncryptionAtRestOptions": {
        "Enabled": boolean,
        "KmsKeyId": "string"
      },
      "EngineVersion": "string",
      "Id": "string",
      "LogPublishingOptions": {
        "AuditLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
        },
        "IndexSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
        },
        "SearchSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
        }
      },
      "NodeToNodeEncryptionOptions": {
        "Enabled": boolean
```

```
        },
        "ServiceSoftwareOptions": {
         "AutomatedUpdateDate": "string",
         "Cancellable": boolean,
         "CurrentVersion": "string",
         "Description": "string",
         "NewVersion": "string",
         "OptionalDeployment": boolean,
         "UpdateAvailable": boolean,
         "UpdateStatus": "string"
        },
        "VpcOptions": {
         "SecurityGroupIds": ["string"],
         "SubnetIds": ["string"]
        }
       },
       "AwsRdsDbCluster": {
        "ActivityStreamStatus": "string",
        "AllocatedStorage": number,
        "AssociatedRoles": [{
         "RoleArn": "string",
         "Status": "string"
        }],
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZones": ["string"],
        "BackupRetentionPeriod": integer,
        "ClusterCreateTime": "string",
        "CopyTagsToSnapshot": boolean,
        "CrossAccountClone": boolean,
        "CustomEndpoints": ["string"],
        "DatabaseName": "string",
        "DbClusterIdentifier": "string",
        "DbClusterMembers": [{
         "DbClusterParameterGroupStatus": "string",
         "DbInstanceIdentifier": "string",
         "IsClusterWriter": boolean,
         "PromotionTier": integer
        }],
        "DbClusterOptionGroupMemberships": [{
         "DbClusterOptionGroupName": "string",
         "Status": "string"
        }],
        "DbClusterParameterGroup": "string",
        "DbClusterResourceId": "string",
```

```
        "DbSubnetGroup": "string",
        "DeletionProtection": boolean,
        "DomainMemberships": [{
         "Domain": "string",
         "Fqdn": "string",
         "IamRoleName": "string",
         "Status": "string"
        }],
        "EnabledCloudwatchLogsExports": ["string"],
        "Endpoint": "string",
        "Engine": "string",
        "EngineMode": "string",
        "EngineVersion": "string",
        "HostedZoneId": "string",
        "HttpEndpointEnabled": boolean,
        "IamDatabaseAuthenticationEnabled": boolean,
        "KmsKeyId": "string",
        "MasterUsername": "string",
        "MultiAz": boolean,
        "Port": integer,
        "PreferredBackupWindow": "string",
        "PreferredMaintenanceWindow": "string",
        "ReaderEndpoint": "string",
        "ReadReplicaIdentifiers": ["string"],
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcSecurityGroups": [{
         "Status": "string",
         "VpcSecurityGroupId": "string"
        }]
       },
       "AwsRdsDbClusterSnapshot": {
        "AllocatedStorage": integer,
        "AvailabilityZones": ["string"],
        "ClusterCreateTime": "string",
        "DbClusterIdentifier": "string",
        "DbClusterSnapshotAttributes": [{
         "AttributeName": "string",
         "AttributeValues": ["string"]
        }],
        "DbClusterSnapshotIdentifier": "string",
        "Engine": "string",
        "EngineVersion": "string",
        "IamDatabaseAuthenticationEnabled": boolean,
```

```
        "KmsKeyId": "string",
        "LicenseModel": "string",
        "MasterUsername": "string",
        "PercentProgress": integer,
        "Port": integer,
        "SnapshotCreateTime": "string",
        "SnapshotType": "string",
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcId": "string"
       },
       "AwsRdsDbInstance": {
        "AllocatedStorage": number,
        "AssociatedRoles": [{
         "RoleArn": "string",
         "FeatureName": "string",
         "Status": "string"
        }],
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZone": "string",
        "BackupRetentionPeriod": number,
        "CACertificateIdentifier": "string",
        "CharacterSetName": "string",
        "CopyTagsToSnapshot": boolean,
        "DBClusterIdentifier": "string",
        "DBInstanceClass": "string",
        "DBInstanceIdentifier": "string",
        "DbInstancePort": number,
        "DbInstanceStatus": "string",
        "DbiResourceId": "string",
        "DBName": "string",
        "DbParameterGroups": [{
         "DbParameterGroupName": "string",
         "ParameterApplyStatus": "string"
        }],
        "DbSecurityGroups": ["string"],
        "DbSubnetGroup": {
         "DbSubnetGroupArn": "string",
         "DbSubnetGroupDescription": "string",
         "DbSubnetGroupName": "string",
         "SubnetGroupStatus": "string",
         "Subnets": [{
          "SubnetAvailabilityZone": {
           "Name": "string"
```

```
        },
        "SubnetIdentifier": "string",
        "SubnetStatus": "string"
       }],
       "VpcId": "string"
      },
      "DeletionProtection": boolean,
      "Endpoint": {
       "Address": "string",
       "Port": number,
       "HostedZoneId": "string"
      },
      "DomainMemberships": [{
       "Domain": "string",
       "Fqdn": "string",
       "IamRoleName": "string",
       "Status": "string"
      }],
      "EnabledCloudwatchLogsExports": ["string"],
      "Engine": "string",
      "EngineVersion": "string",
      "EnhancedMonitoringResourceArn": "string",
      "IAMDatabaseAuthenticationEnabled": boolean,
      "InstanceCreateTime": "string",
      "Iops": number,
      "KmsKeyId": "string",
      "LatestRestorableTime": "string",
      "LicenseModel": "string",
      "ListenerEndpoint": {
       "Address": "string",
       "HostedZoneId": "string",
       "Port": number
      },
      "MasterUsername": "admin",
      "MaxAllocatedStorage": number,
      "MonitoringInterval": number,
      "MonitoringRoleArn": "string",
      "MultiAz": boolean,
      "OptionGroupMemberships": [{
       "OptionGroupName": "string",
       "Status": "string"
      }],
      "PendingModifiedValues": {
       "AllocatedStorage": number,
```

```
        "BackupRetentionPeriod": number,
        "CaCertificateIdentifier": "string",
        "DbInstanceClass": "string",
        "DbInstanceIdentifier": "string",
        "DbSubnetGroupName": "string",
        "EngineVersion": "string",
        "Iops": number,
        "LicenseModel": "string",
        "MasterUserPassword": "string",
        "MultiAZ": boolean,
        "PendingCloudWatchLogsExports": {
         "LogTypesToDisable": ["string"],
         "LogTypesToEnable": ["string"]
        },
        "Port": number,
        "ProcessorFeatures": [{
         "Name": "string",
         "Value": "string"
        }],
        "StorageType": "string"
       },
       "PerformanceInsightsEnabled": boolean,
       "PerformanceInsightsKmsKeyId": "string",
       "PerformanceInsightsRetentionPeriod": number,
       "PreferredBackupWindow": "string",
       "PreferredMaintenanceWindow": "string",
       "ProcessorFeatures": [{
        "Name": "string",
        "Value": "string"
       }],
       "PromotionTier": number,
       "PubliclyAccessible": boolean,
       "ReadReplicaDBClusterIdentifiers": ["string"],
       "ReadReplicaDBInstanceIdentifiers": ["string"],
       "ReadReplicaSourceDBInstanceIdentifier": "string",
       "SecondaryAvailabilityZone": "string",
       "StatusInfos": [{
        "Message": "string",
        "Normal": boolean,
        "Status": "string",
        "StatusType": "string"
       }],
       "StorageEncrypted": boolean,
       "TdeCredentialArn": "string",
```

```
        "Timezone": "string",
        "VpcSecurityGroups": [{
         "VpcSecurityGroupId": "string",
         "Status": "string"
        }]
       },
       "AwsRdsDbSecurityGroup": {
        "DbSecurityGroupArn": "string",
        "DbSecurityGroupDescription": "string",
        "DbSecurityGroupName": "string",
        "Ec2SecurityGroups": [{
         "Ec2SecurityGroupuId": "string",
         "Ec2SecurityGroupName": "string",
         "Ec2SecurityGroupOwnerId": "string",
         "Status": "string"
        }],
        "IpRanges": [{
         "CidrIp": "string",
         "Status": "string"
        }],
        "OwnerId": "string",
        "VpcId": "string"
       },
       "AwsRdsDbSnapshot": {
        "AllocatedStorage": integer,
        "AvailabilityZone": "string",
        "DbInstanceIdentifier": "string",
        "DbiResourceId": "string",
        "DbSnapshotIdentifier": "string",
        "Encrypted": boolean,
        "Engine": "string",
        "EngineVersion": "string",
        "IamDatabaseAuthenticationEnabled": boolean,
        "InstanceCreateTime": "string",
        "Iops": number,
        "KmsKeyId": "string",
        "LicenseModel": "string",
        "MasterUsername": "string",
        "OptionGroupName": "string",
        "PercentProgress": integer,
        "Port": integer,
        "ProcessorFeatures": [],
        "SnapshotCreateTime": "string",
        "SnapshotType": "string",
```

```
        "SourceDbSnapshotIdentifier": "string",
        "SourceRegion": "string",
        "Status": "string",
        "StorageType": "string",
        "TdeCredentialArn": "string",
        "Timezone": "string",
        "VpcId": "string"
      },
      "AwsRdsEventSubscription": {
        "CustomerAwsId": "string",
        "CustSubscriptionId": "string",
        "Enabled": boolean,
        "EventCategoriesList": ["string"],
        "EventSubscriptionArn": "string",
        "SnsTopicArn": "string",
        "SourceIdsList": ["string"],
        "SourceType": "string",
        "Status": "string",
        "SubscriptionCreationTime": "string"
      },
      "AwsRedshiftCluster": {
        "AllowVersionUpgrade": boolean,
        "AutomatedSnapshotRetentionPeriod": number,
        "AvailabilityZone": "string",
        "ClusterAvailabilityStatus": "string",
        "ClusterCreateTime": "string",
        "ClusterIdentifier": "string",
        "ClusterNodes": [{
          "NodeRole": "string",
          "PrivateIPAddress": "string",
          "PublicIPAddress": "string"
        }],
        "ClusterParameterGroups": [{
          "ClusterParameterStatusList": [{
            "ParameterApplyErrorDescription": "string",
            "ParameterApplyStatus": "string",
            "ParameterName": "string"
          }],
          "ParameterApplyStatus": "string",
          "ParameterGroupName": "string"
        }],
        "ClusterPublicKey": "string",
        "ClusterRevisionNumber": "string",
        "ClusterSecurityGroups": [{
```

```
        "ClusterSecurityGroupName": "string",
        "Status": "string"
      }],
      "ClusterSnapshotCopyStatus": {
        "DestinationRegion": "string",
        "ManualSnapshotRetentionPeriod": number,
        "RetentionPeriod": number,
        "SnapshotCopyGrantName": "string"
      },
      "ClusterStatus": "string",
      "ClusterSubnetGroupName": "string",
      "ClusterVersion": "string",
      "DBName": "string",
      "DeferredMaintenanceWindows": [{
        "DeferMaintenanceEndTime": "string",
        "DeferMaintenanceIdentifier": "string",
        "DeferMaintenanceStartTime": "string"
      }],
      "ElasticIpStatus": {
        "ElasticIp": "string",
        "Status": "string"
      },
      "ElasticResizeNumberOfNodeOptions": "string",
      "Encrypted": boolean,
      "Endpoint": {
        "Address": "string",
        "Port": number
      },
      "EnhancedVpcRouting": boolean,
      "ExpectedNextSnapshotScheduleTime": "string",
      "ExpectedNextSnapshotScheduleTimeStatus": "string",
      "HsmStatus": {
        "HsmClientCertificateIdentifier": "string",
        "HsmConfigurationIdentifier": "string",
        "Status": "string"
      },
      "IamRoles": [{
        "ApplyStatus": "string",
        "IamRoleArn": "string"
      }],
      "KmsKeyId": "string",
      "LoggingStatus":{
                  "BucketName": "string",
                  "LastFailureMessage": "string",
```

```
                "LastFailureTime": "string",
                "LastSuccessfulDeliveryTime": "string",
                "LoggingEnabled": boolean,
                "S3KeyPrefix": "string"
            },
        "MaintenanceTrackName": "string",
        "ManualSnapshotRetentionPeriod": number,
        "MasterUsername": "string",
        "NextMaintenanceWindowStartTime": "string",
        "NodeType": "string",
        "NumberOfNodes": number,
        "PendingActions": ["string"],
        "PendingModifiedValues": {
         "AutomatedSnapshotRetentionPeriod": number,
         "ClusterIdentifier": "string",
         "ClusterType": "string",
         "ClusterVersion": "string",
         "EncryptionType": "string",
         "EnhancedVpcRouting": boolean,
         "MaintenanceTrackName": "string",
         "MasterUserPassword": "string",
         "NodeType": "string",
         "NumberOfNodes": number,
         "PubliclyAccessible": "string"
        },
        "PreferredMaintenanceWindow": "string",
        "PubliclyAccessible": boolean,
        "ResizeInfo": {
         "AllowCancelResize": boolean,
         "ResizeType": "string"
        },
        "RestoreStatus": {
         "CurrentRestoreRateInMegaBytesPerSecond": number,
         "ElapsedTimeInSeconds": number,
         "EstimatedTimeToCompletionInSeconds": number,
         "ProgressInMegaBytes": number,
         "SnapshotSizeInMegaBytes": number,
         "Status": "string"
        },
        "SnapshotScheduleIdentifier": "string",
        "SnapshotScheduleState": "string",
        "VpcId": "string",
        "VpcSecurityGroups": [{
         "Status": "string",
```

```
        "VpcSecurityGroupId": "string"
       }]
      },
      "AwsRoute53HostedZone": {
       "HostedZone": {
        "Id": "string",
        "Name": "string",
        "Config": {
         "Comment": "string"
        }
       },
       "NameServers": ["string"],
       "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
         "CloudWatchLogsLogGroupArn": "string",
         "Id": "string",
         "HostedZoneId": "string"
        }
       },
       "Vpcs": [
        {
         "Id": "string",
         "Region": "string"
        }
       ]
      },
      "AwsS3AccessPoint": {
       "AccessPointArn": "string",
       "Alias": "string",
       "Bucket": "string",
       "BucketAccountId": "string",
       "Name": "string",
       "NetworkOrigin": "string",
       "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": boolean,
        "BlockPublicPolicy": boolean,
        "IgnorePublicAcls": boolean,
        "RestrictPublicBuckets": boolean
       },
       "VpcConfiguration": {
        "VpcId": "string"
       }
      },
      "AwsS3AccountPublicAccessBlock": {
```

```
        "BlockPublicAcls": boolean,
        "BlockPublicPolicy": boolean,
        "IgnorePublicAcls": boolean,
        "RestrictPublicBuckets": boolean
      },
      "AwsS3Bucket": {
        "AccessControlList": "string",
        "BucketLifecycleConfiguration": {
          "Rules": [{
            "AbortIncompleteMultipartUpload": {
              "DaysAfterInitiation": number
            },
            "ExpirationDate": "string",
            "ExpirationInDays": number,
            "ExpiredObjectDeleteMarker": boolean,
            "Filter": {
              "Predicate": {
                "Operands": [{
                  "Prefix": "string",
                  "Type": "string"
                },
                {
                  "Tag": {
                    "Key": "string",
                    "Value": "string"
                  },
                  "Type": "string"
                }
              ],
              "Type": "string"
            }
          },
          "Id": "string",
          "NoncurrentVersionExpirationInDays": number,
          "NoncurrentVersionTransitions": [{
            "Days": number,
            "StorageClass": "string"
          }],
          "Prefix": "string",
          "Status": "string",
          "Transitions": [{
            "Date": "string",
            "Days": number,
            "StorageClass": "string"
```

```
          }]
         }]
        },
        "BucketLoggingConfiguration": {
         "DestinationBucketName": "string",
         "LogFilePrefix": "string"
        },
        "BucketName": "string",
        "BucketNotificationConfiguration": {
         "Configurations": [{
          "Destination": "string",
          "Events": ["string"],
          "Filter": {
           "S3KeyFilter": {
            "FilterRules": [{
             "Name": "string",
             "Value": "string"
            }]
           }
          },
          "Type": "string"
         }]
        },
        "BucketVersioningConfiguration": {
         "IsMfaDeleteEnabled": boolean,
         "Status": "string"
        },
        "BucketWebsiteConfiguration": {
         "ErrorDocument": "string",
         "IndexDocumentSuffix": "string",
         "RedirectAllRequestsTo": {
          "HostName": "string",
          "Protocol": "string"
         },
         "RoutingRules": [{
          "Condition": {
           "HttpErrorCodeReturnedEquals": "string",
           "KeyPrefixEquals": "string"
          },
          "Redirect": {
           "HostName": "string",
           "HttpRedirectCode": "string",
           "Protocol": "string",
           "ReplaceKeyPrefixWith": "string",
```

```
          "ReplaceKeyWith": "string"
         }
        }]
       },
       "CreatedAt": "string",
       "ObjectLockConfiguration": {
        "ObjectLockEnabled": "string",
        "Rule": {
         "DefaultRetention": {
          "Days": integer,
          "Mode": "string",
          "Years": integer
         }
        }
       },
       "OwnerAccountId": "string",
       "OwnerId": "string",
       "OwnerName": "string",
       "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": boolean,
        "BlockPublicPolicy": boolean,
        "IgnorePublicAcls": boolean,
        "RestrictPublicBuckets": boolean
       },
       "ServerSideEncryptionConfiguration": {
        "Rules": [{
         "ApplyServerSideEncryptionByDefault": {
          "KMSMasterKeyID": "string",
          "SSEAlgorithm": "string"
         }
        }]
       }
      },
      "AwsS3Object": {
       "ContentType": "string",
       "ETag": "string",
       "LastModified": "string",
       "ServerSideEncryption": "string",
       "SSEKMSKeyId": "string",
       "VersionId": "string"
      },
      "AwsSagemakerNotebookInstance": {
       "DirectInternetAccess": "string",
       "InstanceMetadataServiceConfiguration": {
```

```
        "MinimumInstanceMetadataServiceVersion": "string"
       },
       "InstanceType": "string",
       "LastModifiedTime": "string",
       "NetworkInterfaceId": "string",
       "NotebookInstanceArn": "string",
       "NotebookInstanceName": "string",
       "NotebookInstanceStatus": "string",
       "PlatformIdentifier": "string",
       "RoleArn": "string",
       "RootAccess": "string",
       "SecurityGroups": ["string"],
       "SubnetId": "string",
       "Url": "string",
       "VolumeSizeInGB": number
      },
      "AwsSecretsManagerSecret": {
       "Deleted": boolean,
       "Description": "string",
       "KmsKeyId": "string",
       "Name": "string",
       "RotationEnabled": boolean,
       "RotationLambdaArn": "string",
       "RotationOccurredWithinFrequency": boolean,
       "RotationRules": {
        "AutomaticallyAfterDays": integer
       }
      },
      "AwsSnsTopic": {
       "ApplicationSuccessFeedbackRoleArn": "string",
       "FirehoseFailureFeedbackRoleArn": "string",
       "FirehoseSuccessFeedbackRoleArn": "string",
       "HttpFailureFeedbackRoleArn": "string",
       "HttpSuccessFeedbackRoleArn": "string",
       "KmsMasterKeyId": "string",
       "Owner": "string",
       "SqsFailureFeedbackRoleArn": "string",
       "SqsSuccessFeedbackRoleArn": "string",
       "Subscription": {
        "Endpoint": "string",
        "Protocol": "string"
       },
       "TopicName": "string"
      },
```

```
      "AwsSqsQueue": {
       "DeadLetterTargetArn": "string",
       "KmsDataKeyReusePeriodSeconds": number,
       "KmsMasterKeyId": "string",
       "QueueName": "string"
      },
      "AwsSsmPatchCompliance": {
       "Patch": {
        "ComplianceSummary": {
         "ComplianceType": "string",
         "CompliantCriticalCount": integer,
         "CompliantHighCount": integer,
         "CompliantInformationalCount": integer,
         "CompliantLowCount": integer,
         "CompliantMediumCount": integer,
         "CompliantUnspecifiedCount": integer,
         "ExecutionType": "string",
         "NonCompliantCriticalCount": integer,
         "NonCompliantHighCount": integer,
         "NonCompliantInformationalCount": integer,
         "NonCompliantLowCount": integer,
         "NonCompliantMediumCount": integer,
         "NonCompliantUnspecifiedCount": integer,
         "OverallSeverity": "string",
         "PatchBaselineId": "string",
         "PatchGroup": "string",
         "Status": "string"
        }
       }
      },
      "AwsStepFunctionStateMachine": {
       "StateMachineArn": "string",
       "Name": "string",
       "Status": "string",
       "RoleArn": "string",
       "Type": "string",
       "LoggingConfiguration": {
        "Level": "string",
        "IncludeExecutionData": boolean
       },
       "TracingConfiguration": {
        "Enabled": boolean
       }
      },
```

```
      "AwsWafRateBasedRule": {
       "MatchPredicates": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
       }],
       "MetricName": "string",
       "Name": "string",
       "RateKey": "string",
       "RateLimit": number,
       "RuleId": "string"
      },
      "AwsWafRegionalRateBasedRule": {
       "MatchPredicates": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
       }],
       "MetricName": "string",
       "Name": "string",
       "RateKey": "string",
       "RateLimit": number,
       "RuleId": "string"
      },
      "AwsWafRegionalRule": {
       "MetricName": "string",
       "Name": "string",
       "RuleId": "string",
       "PredicateList": [{
           "DataId": "string",
           "Negated": boolean,
           "Type": "string"
       }]
      },
      "AwsWafRegionalRuleGroup": {
       "MetricName": "string",
       "Name": "string",
       "RuleGroupId": "string",
       "Rules": [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
```

```
        "Type": "string"
       }]
      },
      "AwsWafRegionalWebAcl": {
       "DefaultAction": "string",
       "MetricName" : "string",
       "Name": "string",
       "RulesList" : [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string",
        "ExcludedRules": [{
         "ExclusionType": "string",
         "RuleId": "string"
        }],
        "OverrideAction": {
         "Type": "string"
        }
       }],
       "WebAclId": "string"
      },
      "AwsWafRule": {
       "MetricName": "string",
       "Name": "string",
       "PredicateList": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
       }],
       "RuleId": "string"
      },
      "AwsWafRuleGroup": {
       "MetricName": "string",
       "Name": "string",
       "RuleGroupId": "string",
       "Rules": [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
```

```
        "Type": "string"
       }]
      },
      "AwsWafv2RuleGroup": {
       "Arn": "string",
       "Capacity": number,
       "Description": "string",
       "Id": "string",
       "Name": "string",
       "Rules": [{
        "Action": {
        "Allow": {
         "CustomRequestHandling": {
          "InsertHeaders": [
           {
           "Name": "string",
           "Value": "string"
           },
           {
           "Name": "string",
           "Value": "string"
           }
          ]
         }
        }
        },
        "Name": "string",
        "Priority": number,
        "VisibilityConfig": {
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string",
         "SampledRequestsEnabled": boolean
        }
       }],
       "VisibilityConfig": {
        "CloudWatchMetricsEnabled": boolean,
        "MetricName": "string",
        "SampledRequestsEnabled": boolean
       }
      },
      "AwsWafWebAcl": {
       "DefaultAction": "string",
       "Name": "string",
       "Rules": [{
```

```
        "Action": {
         "Type": "string"
        },
        "ExcludedRules": [{
         "RuleId": "string"
        }],
        "OverrideAction": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string"
       }],
       "WebAclId": "string"
      },
      "AwsWafv2WebAcl": {
       "Arn": "string",
       "Capacity": number,
       "CaptchaConfig": {
        "ImmunityTimeProperty": {
         "ImmunityTime": number
        }
       },
       "DefaultAction": {
        "Block": {}
       },
       "Description": "string",
       "ManagedbyFirewallManager": boolean,
       "Name": "string",
       "Rules": [{
        "Action": {
         "RuleAction": {
          "Block": {}
         }
        },
        "Name": "string",
        "Priority": number,
        "VisibilityConfig": {
         "SampledRequestsEnabled": boolean,
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string"
        }
       }],
       "VisibilityConfig": {
```

```
        "SampledRequestsEnabled": boolean,
        "CloudWatchMetricsEnabled": boolean,
        "MetricName": "string"
       }
      },
      "AwsXrayEncryptionConfig": {
       "KeyId": "string",
       "Status": "string",
       "Type": "string"
      },
      "Container": {
       "ContainerRuntime": "string",
       "ImageId": "string",
       "ImageName": "string",
       "LaunchedAt": "string",
       "Name": "string",
       "Privileged": boolean,
       "VolumeMounts": [{
        "Name": "string",
        "MountPath": "string"
       }]
      },
      "Other": {
       "string": "string"
      },
      "Id": "string",
      "Partition": "string",
      "Region": "string",
      "ResourceRole": "string",
      "Tags": {
       "string": "string"
      },
      "Type": "string"
     }],
     "SchemaVersion": "string",
     "Severity": {
      "Label": "string",
      "Normalized": number,
      "Original": "string"
     },
     "Sample": boolean,
     "SourceUrl": "string",
     "Threats": [{
      "FilePaths": [{
```

```
        "FileName": "string",
        "FilePath": "string",
        "Hash": "string",
        "ResourceId": "string"
       }],
       "ItemCount": number,
       "Name": "string",
       "Severity": "string"
      }],
      "ThreatIntelIndicators": [{
       "Category": "string",
       "LastObservedAt": "string",
       "Source": "string",
       "SourceUrl": "string",
       "Type": "string",
       "Value": "string"
      }],
      "Title": "string",
      "Types": ["string"],
      "UpdatedAt": "string",
      "UserDefinedFields": {
       "string": "string"
      },
      "VerificationState": "string",
      "Vulnerabilities": [{
       "CodeVulnerabilities": [{
        "Cwes": [
         "string",
         "string"
        ],
        "FilePath": {
         "EndLine": integer,
         "FileName": "string",
         "FilePath": "string",
         "StartLine": integer
        },
        "SourceArn":"string"
       }],
       "Cvss": [{
        "Adjustments": [{
         "Metric": "string",
         "Reason": "string"
        }],
        "BaseScore": number,
```

```
        "BaseVector": "string",
        "Source": "string",
        "Version": "string"
       }],
       "EpssScore": number,
       "ExploitAvailable": "string",
       "FixAvailable": "string",
       "Id": "string",
       "LastKnownExploitAt": "string",
       "ReferenceUrls": ["string"],
       "RelatedVulnerabilities": ["string"],
       "Vendor": {
        "Name": "string",
        "Url": "string",
        "VendorCreatedAt": "string",
        "VendorSeverity": "string",
        "VendorUpdatedAt": "string"
       },
       "VulnerablePackages": [{
        "Architecture": "string",
        "Epoch": "string",
        "FilePath": "string",
        "FixedInVersion": "string",
        "Name": "string",
        "PackageManager": "string",
        "Release": "string",
        "Remediation": "string",
        "SourceLayerArn": "string",
        "SourceLayerHash": "string",
        "Version": "string"
       }]
      }],
      "Workflow": {
       "Status": "string"
      },
      "WorkflowState": "string"
     }
]
```

Impacto da consolidação nos campos e valores do ASFF

O Security Hub oferece dois tipos de consolidação:

- Visualização consolidada de controles (sempre ativada; não pode ser desativada) — Cada controle tem um único identificador em todos os padrões. A página Controles do console do Security Hub mostra todos os seus controles em todos os padrões.
- Descobertas de controle consolidadas (podem ser ativadas ou desativadas): quando as descobertas de controle consolidadas são ativadas, o Security Hub produz uma única descoberta para uma verificação de segurança, mesmo quando uma verificação é compartilhada em vários padrões. O objetivo é reduzir o ruído da descoberta. Por padrão, as descobertas de controle consolidadas estão ativadas para você se você tiver ativado o Security Hub em ou após 23 de fevereiro de 2023. Caso contrário, são desativadas por padrão. Entretanto, as descobertas de controle consolidadas são ativadas nas contas dos membros do Security Hub somente se estiverem ativadas na conta do administrador. Se o atributo estiver desativado na conta do administrador, ele será desativado nas contas dos membros. Para obter instruções sobre como ativar esse recurso, consulteAtivar/desativar descobertas de controle consolidadas.

Ambos os recursos trazem alterações para os campos e valores de descobertas de controle em AWS Formato de descoberta de segurança (ASFF). Esta seção resume essas alterações.

Visualização de controles consolidados — alterações no ASFF

O recurso de visualização de controles consolidados introduziu as seguintes alterações para controlar a localização de campos e valores no ASFF.

Se seus fluxos de trabalho não dependem dos valores desses campos de descobertas de controle, nenhuma ação é necessária.

Se você tiver fluxos de trabalho que dependem dos valores específicos desses campos de localização de controle, atualize seus fluxos de trabalho para usar os valores atuais.

Campo do ASFF	Valor de exemplo antes da visualização dos controles consolidados	Valor de exemplo após a visualização dos controles consolidados, além da descrição da alteração
Conformidade. SecurityControlId	Não aplicável (campo novo)	EC2.2

Campo do ASFF	Valor de exemplo antes da visualização dos controles consolidados	Valor de exemplo após a visualização dos controles consolidados, além da descrição da alteração
		Apresenta um único ID de controle em todos os padrões. `ProductFields.RuleId` ainda fornece o ID de controle baseado em padrão para controles CIS v1.2.0. `ProductFields.ControlId` ainda fornece o ID de controle baseado em padrões para controles em outros padrões.
Conformidade. AssociatedStandards	Não aplicável (campo novo)	[{" StandardsId ": "padrões/ aws-foundational-security-best - práticas/v/1.0.0"}] Mostra em quais padrões um controle está habilitado.

Campo do ASFF	Valor de exemplo antes da visualização dos controles consolidados	Valor de exemplo após a visualização dos controles consolidados, além da descrição da alteração
ProductFields. ArchivalReasons:0/Descrição	Não aplicável (campo novo)	“A descoberta está em um estado ARCHIVED porque as descobertas de controle consolidadas foram ativadas ou desativadas. Isso faz com que as descobertas no estado anterior sejam arquivadas quando novas descobertas estão sendo geradas.” Descreve por que o Security Hub arquivou as descobertas existentes.
ProductFields. ArchivalReasons:0/ ReasonCode	Não aplicável (campo novo)	"CONSOLIDATED_CONTROL_FINDINGS_UPDATE" Fornece o motivo pelo qual o Security Hub arquivou as descobertas existentes.

Campo do ASFF	Valor de exemplo antes da visualização dos controles consolidados	Valor de exemplo após a visualização dos controles consolidados, além da descrição da alteração
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Esse campo não faz mais referência a um padrão.
Remediation.Recommendation.Text	“Para obter instruções sobre como corrigir esse problema, consulte a documentação do PCI DSS do AWS Security Hub.”	“Para obter instruções sobre como corrigir esse problema, consulte a documentação de controles do AWS Security Hub.” Esse campo não faz mais referência a um padrão.
Remediation.Recommendation.Url	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Esse campo não faz mais referência a um padrão.

Descobertas de controle consolidadas — Alterações no ASFF

Se você ativar as descobertas de controle consolidadas, poderá ser afetado pelas seguintes alterações nos campos e valores de descobertas de controle no ASFF. Essas alterações são adicionais às alterações descritas anteriormente para a visualização de controles consolidados.

Se seus fluxos de trabalho não dependem dos valores desses campos de descobertas de controle, nenhuma ação é necessária.

Se você tiver fluxos de trabalho que dependem dos valores específicos desses campos de localização de controle, atualize seus fluxos de trabalho para usar os valores atuais.

> **Note**
>
> O Automated Security Response na AWS v2.0.0 oferece suporte a descobertas consolidadas de controle. Se você usar essa versão da solução, poderá manter seus fluxos de trabalho ao ativar as descobertas de controle consolidadas.

Campo do ASFF	Valor de exemplo antes de ativar as descobertas de controle consolidadas	Valor de exemplo após ativar as descobertas de controle consolidadas e descrição da alteração
GeneratorId	aws-foundational-security-best-Práticas/V/1.0.0/config.1	security-control/Config.1 Esse campo não faz mais referência a um padrão.
Cargo	O PCI.config.1 deve estar ativado AWS Config	AWS Config deve ser habilitado Esse campo não faz mais referência a informações específicas do padrão.
Id	arn:aws:securityhub:eu-central-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.IAM.5/findi	arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/ab6d6a26-a156-48f0-9403-115983e5a956

Campo do ASFF	Valor de exemplo antes de ativar as descobertas de controle consolidadas	Valor de exemplo após ativar as descobertas de controle consolidadas e descrição da alteração
	ng/ab6d6a26-a156-48f0-9403-115983e5a956	Esse campo não faz mais referência a um padrão.
ProductFields.ControlId	PCI.EC2.2	Removido. Consulte `Compliance.SecurityControlId` em vez disso. Esse campo foi removido em favor de um único ID de controle independente do padrão.
ProductFields.RuleId	1.3	Removido. Consulte `Compliance.SecurityControlId` em vez disso. Esse campo foi removido em favor de um único ID de controle independente do padrão.
Descrição	Esse controle PCI DSS verifica se AWS Config está habilitado na conta atual e na região.	Esse AWS controle verifica se AWS Config está ativado na conta atual e na região. Esse campo não faz mais referência a um padrão.

Campo do ASFF	Valor de exemplo antes de ativar as descobertas de controle consolidadas	Valor de exemplo após ativar as descobertas de controle consolidadas e descrição da alteração

Gravidade	"Severidade": {
	"Product": 90,
	"Etiqueta": "CRÍTICO",
	"Normalizado": 90,
	"Original": "CRÍTICO"
	}
		"Severidade": {
		"Etiqueta": "CRÍTICO",
		"Normalizado": 90,
		"Original": "CRÍTICO"
		}
		O Security Hub não usa mais o campo Produto para descrever a gravidade de uma descoberta.

Tipos	["Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"]	["Software and Configuration Checks/Industry and Regulatory Standards"] Esse campo não faz mais referência a um padrão.
Conformidade. RelatedRequirements	["PCI DSS 10.5.2", “PCI DSS 11.5", “ AWS Fundamentos da CEI 2.5"]	["PCI DSS v3.2.1/10.5.2", "PCI DSS v3.2.1/11.5", “Referência do CIS AWS Foundations v1.2.0/2.5"] Esse campo mostra os requisitos relacionados em todos os padrões habilitados.

Campo do ASFF	Valor de exemplo antes de ativar as descobertas de controle consolidadas	Valor de exemplo após ativar as descobertas de controle consolidadas e descrição da alteração
CreatedAt	2022-05-05T08:18:13.138Z	2022-09-25T08:18:13.138Z O formato permanece o mesmo, mas o valor é redefinido quando você ativa as descobertas de controle consolidadas.
FirstObservedAt	2022-05-07T08:18:13.138Z	2022-09-28T08:18:13.138Z O formato permanece o mesmo, mas o valor é redefinido quando você ativa as descobertas de controle consolidadas.
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation	Removido. Consulte `Remediation.Recommendation.Url` em vez disso.
ProductFields.StandardsArn	arn: aws:securityhub: ::standards/ -practices/v/1.0.0 aws-foundational-security-best	Removido. Consulte `Compliance.AssociatedStandards` em vez disso.
ProductFields.StandardsControlArn	arn:aws:securityhub:us-east - 1:123456789012:control/ -practices/v/1.0.0/config.1 aws-foundational-security-best	Removido. O Security Hub gera uma descoberta para uma verificação de segurança em todos os padrões.
ProductFields.StandardsGuideArn	arn: aws:securityhub: ::ruleset / /v/1.2.0 cis-aws-foundations-benchmark	Removido. Consulte `Compliance.AssociatedStandards` em vez disso.

Campo do ASFF	Valor de exemplo antes de ativar as descobertas de controle consolidadas	Valor de exemplo após ativar as descobertas de controle consolidadas e descrição da alteração
ProductFields.StandardsGuideSubscriptionArn	arn: aws: hub de segurança: us-east- 2:123456789012: subscriçã o/ /v/1.2.0 cis-aws-foundations-benchmark	Removido. O Security Hub gera uma descoberta para uma verificação de segurança em todos os padrões.
ProductFields.StandardsSubscriptionArn	arn:aws:securityhub:us-east-1:123456789012: subscription/ -practices/v/1.0.0 aws-foundational-security-best	Removido. O Security Hub gera uma descoberta para uma verificação de segurança em todos os padrões.
ProductFields.aws/securityhub/ FindingId	arn:aws:securityhub:us-east-1: :product/aws/securityhub/ arn:aws:securityhub:us-east-1:123456789012:subscription/ -practices/v/1.0.0/config.1/finding/751c2173-7372-4e12-8656-a5210dfb1d67 aws-foundational-security-best	arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/Config.1/finding/751c2173-7372-4e12-8656-a5210dfb1d67 Esse campo não faz mais referência a um padrão.

Valores dos campos ASFF fornecidos pelo cliente após ativar as descobertas de controle consolidadas

Se você ativar as descobertas de controle consolidadas, o Security Hub gerará uma descoberta em todos os padrões e arquivará as descobertas originais (descobertas separadas para cada padrão). Para ver as descobertas arquivadas, é possível visitar a página Descobertas do console do Security Hub com o filtro de Estado do registro definido como ARQUIVADO ou usar a ação da API `GetFindings`. As atualizações que você fez nas descobertas originais no console do Security Hub ou usando a BatchUpdateFindingsAPI não serão preservadas nas novas descobertas (se necessário, você pode recuperar esses dados consultando as descobertas arquivadas).

Campo do ASFF fornecido pelo cliente	Descrição da mudança após ativar as descobertas de controle consolidadas
Confiança	Redefine para o estado vazio.
Criticidade	Redefine para o estado vazio.
Observação	Redefine para o estado vazio.
RelatedFindings	Redefine para o estado vazio.
Gravidade	Severidade padrão da descoberta (correspo nde à severidade do controle).
Tipos	Redefine para o valor independente do padrão.
UserDefinedFields	Redefine para o estado vazio.
VerificationState	Redefine para o estado vazio.
Fluxo de trabalho	Novas descobertas malsucedidas têm um valor padrão de `NEW`. Novas descobertas passadas têm um valor padrão de `RESOLVED`.

IDs do gerador antes e depois de ativar as descobertas de controle consolidadas

Aqui está uma lista de alterações no ID do gerador para controles quando você ativa as descobertas de controle consolidadas. Elas se aplicam aos controles compatíveis com o Security Hub em 15 de fevereiro de 2023.

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.1 cis-aws-foundations-benchmark	controle de segurança/ 1CloudWatch.
arn: aws:securityhub: ::ruleset/ /v/1.2.0/ rule/1.10 cis-aws-foundations-benchmark	security-control/IAM.16

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
arn: aws:securityhub: ::ruleset/ /v/1.2.0/ rule/1.11 cis-aws-foundations-benchmark	security-control/IAM.17
arn: aws:securityhub: ::ruleset/ /v/1.2.0/ rule/1.12 cis-aws-foundations-benchmark	security-control/IAM.4
arn: aws:securityhub: ::ruleset/ /v/1.2.0/ rule/1.13 cis-aws-foundations-benchmark	security-control/IAM.9
arn: aws:securityhub: ::ruleset/ /v/1.2.0/ rule/1.14 cis-aws-foundations-benchmark	security-control/IAM.6
arn: aws:securityhub: ::ruleset/ /v/1.2.0/ rule/1.16 cis-aws-foundations-benchmark	security-control/IAM.2
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.2 cis-aws-foundations-benchmark	security-control/IAM.5
arn: aws:securityhub: ::ruleset/ /v/1.2.0/ rule/1.20 cis-aws-foundations-benchmark	security-control/IAM.18
arn: aws:securityhub: ::ruleset/ /v/1.2.0/ rule/1.22 cis-aws-foundations-benchmark	security-control/IAM.1
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.3 cis-aws-foundations-benchmark	security-control/IAM.8
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.4 cis-aws-foundations-benchmark	security-control/IAM.3
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.5 cis-aws-foundations-benchmark	security-control/IAM.11
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.6 cis-aws-foundations-benchmark	security-control/IAM.12

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.7 cis-aws-foundations-benchmark	security-control/IAM.13
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.8 cis-aws-foundations-benchmark	security-control/IAM.14
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.9 cis-aws-foundations-benchmark	security-control/IAM.15
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.1 cis-aws-foundations-benchmark	controle de segurança/ 1CloudTrail.
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.2 cis-aws-foundations-benchmark	controle de segurança/ 4CloudTrail.
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.3 cis-aws-foundations-benchmark	controle de segurança/ 6CloudTrail.
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.4 cis-aws-foundations-benchmark	controle de segurança/ 5CloudTrail.
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.5 cis-aws-foundations-benchmark	security-control/Config.1
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.6 cis-aws-foundations-benchmark	controle de segurança/ 7CloudTrail.
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.7 cis-aws-foundations-benchmark	controle de segurança/ 2CloudTrail.
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.8 cis-aws-foundations-benchmark	security-control/KMS.4
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.9 cis-aws-foundations-benchmark	security-control/EC2.6

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.1 cis-aws-foundations-benchmark	controle de segurança/ 2CloudWatch.
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.2 cis-aws-foundations-benchmark	controle de segurança/ 3CloudWatch.
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.3 cis-aws-foundations-benchmark	controle de segurança/ 1CloudWatch.
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.4 cis-aws-foundations-benchmark	controle de segurança/ 4CloudWatch.
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.5 cis-aws-foundations-benchmark	controle de segurança/ 5CloudWatch.
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.6 cis-aws-foundations-benchmark	controle de segurança/ 6CloudWatch.
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.7 cis-aws-foundations-benchmark	controle de segurança/ 7CloudWatch.
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.8 cis-aws-foundations-benchmark	controle de segurança/ 8CloudWatch.
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.9 cis-aws-foundations-benchmark	controle de segurança/ 9CloudWatch.
arn: aws:securityhub: ::ruleset/ /v/1.2.0/ rule/3.10 cis-aws-foundations-benchmark	controle de segurança/ .10 CloudWatch
arn: aws:securityhub: ::ruleset/ /v/1.2.0/ rule/3.11 cis-aws-foundations-benchmark	controle de segurança/ 1.1 CloudWatch
arn: aws:securityhub: ::ruleset/ /v/1.2.0/ rule/3.12 cis-aws-foundations-benchmark	controle de segurança/ 1.2 CloudWatch

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
arn: aws:securityhub: ::ruleset/ /v/1.2.0/ rule/3.13 cis-aws-foundations-benchmark	controle de segurança/ 1.3 CloudWatch
arn: aws:securityhub: ::ruleset/ /v/1.2.0/ rule/3.14 cis-aws-foundations-benchmark	controle de segurança/ 1.4 CloudWatch
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/4.1 cis-aws-foundations-benchmark	security-control/EC2.13
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/4.2 cis-aws-foundations-benchmark	security-control/EC2.14
arn: aws:securityhub: ::ruleset/ /v/1.2.0/rule/4.3 cis-aws-foundations-benchmark	security-control/EC2.2
cis-aws-foundations-benchmark/v/1.4.0/1,10	security-control/IAM.5
cis-aws-foundations-benchmark/v/1.4.0/1,14	security-control/IAM.3
cis-aws-foundations-benchmark/v/1.4.0/1,16	security-control/IAM.1
cis-aws-foundations-benchmark/v/1.4.0/1,17	security-control/IAM.18
cis-aws-foundations-benchmark/v/1.4.0/1.4	security-control/IAM.4
cis-aws-foundations-benchmark/v/1.4.0/1,5	security-control/IAM.9
cis-aws-foundations-benchmark/v/1.4.0/1.6	security-control/IAM.6
cis-aws-foundations-benchmark/v/1.4.0/1,7	controle de segurança/ 1CloudWatch.
cis-aws-foundations-benchmark/v/1.4.0/1,8	security-control/IAM.15
cis-aws-foundations-benchmark/v/1.4.0/1,9	security-control/IAM.16
cis-aws-foundations-benchmark/v/1.4.0/2.1.2	security-control/S3.5
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.1	security-control/S3.1

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.2	security-control/S3.8
cis-aws-foundations-benchmark/v/1.4.0/2.2.1	security-control/EC2.7
cis-aws-foundations-benchmark/v/1.4.0/2.3.1	security-control/RDS.3
cis-aws-foundations-benchmark/v/1.4.0/3.1	controle de segurança/ 1CloudTrail.
cis-aws-foundations-benchmark/v/1.4.0/3.2	controle de segurança/ 4CloudTrail.
cis-aws-foundations-benchmark/v/1.4.0/3.4	controle de segurança/ 5CloudTrail.
cis-aws-foundations-benchmark/v/1.4.0/3,5	security-control/Config.1
cis-aws-foundations-benchmark/v/1.4.0/3.6	security-control/S3.9
cis-aws-foundations-benchmark/v/1.4.0/3.7	controle de segurança/ 2CloudTrail.
cis-aws-foundations-benchmark/v/1.4.0/3.8	security-control/KMS.4
cis-aws-foundations-benchmark/v/1.4.0/3.9	security-control/EC2.6
cis-aws-foundations-benchmark/v/1.4.0/4.3	controle de segurança/ 1CloudWatch.
cis-aws-foundations-benchmark/v/1.4.0/4,4	controle de segurança/ 4CloudWatch.
cis-aws-foundations-benchmark/v/1.4.0/4.5	controle de segurança/ 5CloudWatch.
cis-aws-foundations-benchmark/v/1.4.0/4.6	controle de segurança/ 6CloudWatch.
cis-aws-foundations-benchmark/v/1.4.0/4.7	controle de segurança/ 7CloudWatch.
cis-aws-foundations-benchmark/v/1.4.0/4.8	controle de segurança/ 8CloudWatch.
cis-aws-foundations-benchmark/v/1.4.0/4.9	controle de segurança/ 9CloudWatch.
cis-aws-foundations-benchmark/v/1.4.0/4,10	controle de segurança/ .10 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4,11	controle de segurança/ 1.1 CloudWatch

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
cis-aws-foundations-benchmark/v/1.4.0/4,12	controle de segurança/ 1.2 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4,13	controle de segurança/ 1.3 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4,14	controle de segurança/ 1.4 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/5.1	security-control/EC2.21
cis-aws-foundations-benchmark/v/1.4.0/5.3	security-control/EC2.2
aws-foundational-security-best-Práticas/V/1.0.0/Conta.1	security-control/Account.1
aws-foundational-security-best-Práticas/V/1.0.0/ACM.1	security-control/ACM.1
aws-foundational-security-best- Práticas/V/1.0.0/API Gateway.1	security-control/APIGateway.1
aws-foundational-security-best- Práticas/V/1.0.0/API Gateway.2	security-control/APIGateway.2
aws-foundational-security-best- Práticas/V/1.0.0/API Gateway.3	security-control/APIGateway.3
aws-foundational-security-best- Práticas/V/1.0.0/API Gateway.4	security-control/APIGateway.4
aws-foundational-security-best- Práticas/V/1.0.0/API Gateway.5	security-control/APIGateway.5
aws-foundational-security-best- Práticas/V/1.0.0/API Gateway.8	security-control/APIGateway.8
aws-foundational-security-best- Práticas/V/1.0.0/API Gateway.9	security-control/APIGateway.9

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
aws-foundational-security-best-práticas/v/1.0 .0/ .1 AutoScaling	controle de segurança/ 1AutoScaling.
aws-foundational-security-best-práticas/v/1.0 .0/2AutoScaling.	controle de segurança/ 2AutoScaling.
aws-foundational-security-best-práticas/v/1.0 .0/ .3 AutoScaling	controle de segurança/ 3AutoScaling.
aws-foundational-security-best-Práticas/V/1.0 .0/Autoscaling.5	security-control/Autoscaling.5
aws-foundational-security-best-práticas/v/1.0 .0/6AutoScaling.	controle de segurança/ 6AutoScaling.
aws-foundational-security-best-práticas/v/1.0 .0/9AutoScaling.	controle de segurança/ 9AutoScaling.
aws-foundational-security-best-práticas/v/1.0 .0/ .1 CloudFront	controle de segurança/ 1CloudFront.
aws-foundational-security-best-práticas/v/1.0 .0/ .3 CloudFront	controle de segurança/ 3CloudFront.
aws-foundational-security-best-práticas/v/1.0.0/ 1.4 CloudFront	controle de segurança/ 4CloudFront.
aws-foundational-security-best-práticas/v/1.0 .0/5CloudFront.	controle de segurança/ 5CloudFront.
aws-foundational-security-best-práticas/v/1.0 .0/6CloudFront.	controle de segurança/ 6CloudFront.
aws-foundational-security-best-práticas/v/1.0 .0/7CloudFront.	controle de segurança/ 7CloudFront.

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
aws-foundational-security-best-práticas/v/1.0 .0/8CloudFront.	controle de segurança/ 8CloudFront.
aws-foundational-security-best-práticas/v/1.0 .0/9CloudFront.	controle de segurança/ 9CloudFront.
aws-foundational-security-best-práticas/v/1.0.0/ 1.0 CloudFront	controle de segurança/ .10 CloudFront
aws-foundational-security-best-práticas/v/1.0.0/ 1.2 CloudFront	controle de segurança/ 1.2 CloudFront
aws-foundational-security-best-práticas/v/1.0 .0/ .1 CloudTrail	controle de segurança/ 1CloudTrail.
aws-foundational-security-best-práticas/v/1.0 .0/2CloudTrail.	controle de segurança/ 2CloudTrail.
aws-foundational-security-best-práticas/v/1.0.0/ 1.4 CloudTrail	controle de segurança/ 4CloudTrail.
aws-foundational-security-best-práticas/v/1.0 .0/5CloudTrail.	controle de segurança/ 5CloudTrail.
aws-foundational-security-best-práticas/v/1.0 .0/ .1 CodeBuild	controle de segurança/ 1CodeBuild.
aws-foundational-security-best-práticas/v/1.0 .0/2CodeBuild.	controle de segurança/ 2CodeBuild.
aws-foundational-security-best-práticas/v/1.0 .0/ .3 CodeBuild	controle de segurança/ 3CodeBuild.
aws-foundational-security-best-práticas/v/1.0.0/ 1.4 CodeBuild	controle de segurança/ 4CodeBuild.

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
aws-foundational-security-best-Práticas/V/1.0.0/config.1	security-control/Config.1
aws-foundational-security-best-Práticas/V/1.0.0/DMS.1	security-control/DMS.1
aws-foundational-security-best-Práticas/V/1.0.0/DynamoDB.1	security-control/DynamoDB.1
aws-foundational-security-best-Práticas/V/1.0.0/DynamoDB.2	security-control/DynamoDB.2
aws-foundational-security-best-Práticas/V/1.0.0/DynamoDB.3	security-control/DynamoDB.3
aws-foundational-security-best-Práticas/V/1.0.0/EC2.1	security-control/EC2.1
aws-foundational-security-best-Práticas/V/1.0.0/EC2.3	security-control/EC2.3
aws-foundational-security-best-Práticas/V/1.0.0/EC2.4	security-control/EC2.4
aws-foundational-security-best-Práticas/V/1.0.0/EC2.6	security-control/EC2.6
aws-foundational-security-best-Práticas/V/1.0.0/EC2.7	security-control/EC2.7
aws-foundational-security-best-Práticas/V/1.0.0/EC2.8	security-control/EC2.8
aws-foundational-security-best-Práticas/V/1.0.0/EC2.9	security-control/EC2.9

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
aws-foundational-security-best-Práticas/V/1.0.0/EC2.10	security-control/EC2.10
aws-foundational-security-best-Práticas/V/1.0.0/EC2.15	security-control/EC2.15
aws-foundational-security-best-Práticas/V/1.0.0/EC2.16	security-control/EC2.16
aws-foundational-security-best-Práticas/V/1.0.0/EC2.17	security-control/EC2.17
aws-foundational-security-best-Práticas/V/1.0.0/EC2.18	security-control/EC2.18
aws-foundational-security-best-Práticas/V/1.0.0/EC2.19	security-control/EC2.19
aws-foundational-security-best-Práticas/V/1.0.0/EC2.2	security-control/EC2.2
aws-foundational-security-best-Práticas/V/1.0.0/EC2.20	security-control/EC2.20
aws-foundational-security-best-Práticas/V/1.0.0/EC2.21	security-control/EC2.21
aws-foundational-security-best-Práticas/V/1.0.0/EC2.23	security-control/EC2.23
aws-foundational-security-best-Práticas/V/1.0.0/EC2.24	security-control/EC2.24
aws-foundational-security-best-Práticas/V/1.0.0/EC2.25	security-control/EC2.25

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
aws-foundational-security-best-Práticas/V/1.0.0/ECR.1	security-control/ECR.1
aws-foundational-security-best-Práticas/V/1.0.0/ECR.2	security-control/ECR.2
aws-foundational-security-best-Práticas/V/1.0.0/ECr.3	security-control/ECR.3
aws-foundational-security-best-Práticas/V/1.0.0/ECS.1	security-control/ECS.1
aws-foundational-security-best-Práticas/V/1.0.0/ECS.10	security-control/ECS.10
aws-foundational-security-best-Práticas/V/1.0.0/ECS.12	security-control/ECS.12
aws-foundational-security-best-Práticas/V/1.0.0/ECS.2	security-control/ECS.2
aws-foundational-security-best-Práticas/V/1.0.0/ECS.3	security-control/ECS.3
aws-foundational-security-best-Práticas/V/1.0.0/ECS.4	security-control/ECS.4
aws-foundational-security-best-Práticas/V/1.0.0/ECS.5	security-control/ECS.5
aws-foundational-security-best-Práticas/V/1.0.0/ECS.8	security-control/ECS.8
aws-foundational-security-best-Práticas/V/1.0.0/EFS.1	security-control/EFS.1

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
aws-foundational-security-best-Práticas/V/1.0.0/EFS.2	security-control/EFS.2
aws-foundational-security-best-Práticas/V/1.0.0/EFS.3	security-control/EFS.3
aws-foundational-security-best-Práticas/V/1.0.0/EFS.4	security-control/EFS.4
aws-foundational-security-best-Práticas/V/1.0.0/EKS.2	security-control/EKS.2
aws-foundational-security-best-práticas/v/1.0.0/ .1 ElasticBeanstalk	controle de segurança/ 1ElasticBeanstalk.
aws-foundational-security-best-práticas/v/1.0.0/ .2 ElasticBeanstalk	controle de segurança/ 2ElasticBeanstalk.
aws-foundational-security-best-Práticas/V/1.0.0/ELBv2.1	security-control/ELB.1
aws-foundational-security-best-Práticas/V/1.0.0/ELB.2	security-control/ELB.2
aws-foundational-security-best-Práticas/V/1.0.0/ELB.3	security-control/ELB./*
aws-foundational-security-best-Práticas/V/1.0.0/ELB.4	security-control/ELB.4
aws-foundational-security-best-Práticas/V/1.0.0/ELB.5	security-control/ELB.5
aws-foundational-security-best-Práticas/V/1.0.0/ELB.6	security-control/ELB.6

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
aws-foundational-security-best-Práticas/V/1.0.0/ELB.7	security-control/ELB.7
aws-foundational-security-best-Práticas/V/1.0.0/ELB.8	security-control/ELB.8
aws-foundational-security-best-Práticas/V/1.0.0/ELB.9	security-control/ELB.9
aws-foundational-security-best-Práticas/V/1.0.0/ELB.10	security-control/ELB.10
aws-foundational-security-best-Práticas/V/1.0.0/ELB.11	security-control/ELB.11
aws-foundational-security-best-Práticas/V/1.0.0/ELB.12	security-control/ELB.12
aws-foundational-security-best-Práticas/V/1.0.0/ELB.13	security-control/ELB.13
aws-foundational-security-best-Práticas/V/1.0.0/ELB.14	security-control/ELB.14
aws-foundational-security-best-Práticas/V/1.0.0/EMR.1	security-control/EMR.1
aws-foundational-security-best-Práticas/V/1.0.0/ES.1	security-control/ES.1
aws-foundational-security-best-Práticas/V/1.0.0/ES.2	security-control/ES.2
aws-foundational-security-best-Práticas/V/1.0.0/ES.3	security-control/ES.3

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
aws-foundational-security-best-Práticas/V/1.0.0/ES.4	security-control/ES.4
aws-foundational-security-best-Práticas/V/1.0.0/ES.5	security-control/ES.5
aws-foundational-security-best-Práticas/V/1.0.0/ES.6	security-control/ES.6
aws-foundational-security-best-Práticas/V/1.0.0/ES.7	security-control/ES.7
aws-foundational-security-best-Práticas/V/1.0.0/ES.8	security-control/ES.8
aws-foundational-security-best-práticas/v/1.0.0/ .1 GuardDuty	controle de segurança/ 1GuardDuty.
aws-foundational-security-best-Práticas/V/1.0.0/IAM.1	security-control/IAM.1
aws-foundational-security-best-Práticas/V/1.0.0/IAM.2	security-control/IAM.2
aws-foundational-security-best-Práticas/V/1.0.0/IAM.21	security-control/IAM.21
aws-foundational-security-best-Práticas/V/1.0.0/IAM.3	security-control/IAM.3
aws-foundational-security-best-Práticas/V/1.0.0/IAM.4	security-control/IAM.4
aws-foundational-security-best-Práticas/V/1.0.0/IAM.5	security-control/IAM.5

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
aws-foundational-security-best-Práticas/V/1.0.0/IAM.6	security-control/IAM.6
aws-foundational-security-best-Práticas/V/1.0.0/IAM.7	security-control/IAM.7
aws-foundational-security-best-Práticas/V/1.0.0/IAM.8	security-control/IAM.8
aws-foundational-security-best-Práticas/V/1.0.0/Kinesis.1	security-control/Kinesis.1
aws-foundational-security-best-Práticas/V/1.0.0/KMS.1	security-control/KMS.1
aws-foundational-security-best-Práticas/V/1.0.0/KMS.2	security-control/KMS.2
aws-foundational-security-best-Práticas/V/1.0.0/KMS.3	security-control/KMS.3
aws-foundational-security-best-Práticas/V/1.0.0/Lambda.1	security-control/Lambda.1
aws-foundational-security-best-Práticas/V/1.0.0/Lambda.2	security-control/Lambda.2
aws-foundational-security-best-Práticas/V/1.0.0/Lambda.5	security-control/Lambda.5
aws-foundational-security-best-práticas/v/1.0.0/ .3 NetworkFirewall	controle de segurança/ 3NetworkFirewall.
aws-foundational-security-best-práticas/v/1.0.0/ 1.4 NetworkFirewall	controle de segurança/ 4NetworkFirewall.

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
aws-foundational-security-best-práticas/v/1.0.0/5NetworkFirewall.	controle de segurança/ 5NetworkFirewall.
aws-foundational-security-best-práticas/v/1.0.0/6NetworkFirewall.	controle de segurança/ 6NetworkFirewall.
aws-foundational-security-best- Práticas/V/1.0.0/OpenSearch.1	security-control/Opensearch.1
aws-foundational-security-best- Práticas/V/1.0.0/OpenSearch.2	security-control/Opensearch.2
aws-foundational-security-best- Práticas/V/1.0.0/OpenSearch.3	security-control/Opensearch.3
aws-foundational-security-best- Práticas/V/1.0.0/OpenSearch.4	security-control/Opensearch.4
aws-foundational-security-best- Práticas/V/1.0.0/OpenSearch.5	security-control/Opensearch.5
aws-foundational-security-best- Práticas/V/1.0.0/OpenSearch.6	security-control/Opensearch.6
aws-foundational-security-best- Práticas/V/1.0.0/OpenSearch.7	security-control/Opensearch.7
aws-foundational-security-best- Práticas/V/1.0.0/OpenSearch.8	security-control/Opensearch.8
aws-foundational-security-best-Práticas/V/1.0.0/RDS.1	security-control/RDS.1
aws-foundational-security-best-Práticas/V/1.0.0/RDS.10	security-control/RDS.10

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
aws-foundational-security-best-Práticas/V/1.0.0/RDS.11	security-control/RDS.11
aws-foundational-security-best-Práticas/V/1.0.0/RDS.12	security-control/RDS.12
aws-foundational-security-best-Práticas/V/1.0.0/RDS.13	security-control/RDS.13
aws-foundational-security-best-Práticas/V/1.0.0/RDS.14	security-control/RDS.14
aws-foundational-security-best-Práticas/V/1.0.0/RDS.15	security-control/RDS.15
aws-foundational-security-best-Práticas/V/1.0.0/RDS.16	security-control/RDS.16
aws-foundational-security-best-Práticas/V/1.0.0/RDS.17	security-control/RDS.17
aws-foundational-security-best-Práticas/V/1.0.0/RDS.18	security-control/RDS.18
aws-foundational-security-best-Práticas/V/1.0.0/RDS.19	security-control/RDS.19
aws-foundational-security-best-Práticas/V/1.0.0/RDS.2	security-control/RDS.3
aws-foundational-security-best-Práticas/V/1.0.0/RDS.20	security-control/RDS.20
aws-foundational-security-best-Práticas/V/1.0.0/RDS.21	security-control/RDS.21

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
aws-foundational-security-best-Práticas/V/1.0.0/RDS.22	security-control/RDS.22
aws-foundational-security-best-Práticas/V/1.0.0/RDS.23	security-control/RDS.23
aws-foundational-security-best-Práticas/V/1.0.0/RDS.24	security-control/RDS.24
aws-foundational-security-best-Práticas/V/1.0.0/RDS.25	security-control/RDS.25
aws-foundational-security-best-Práticas/V/1.0.0/RDS.3	security-control/RDS.3
aws-foundational-security-best-Práticas/V/1.0.0/RDS.4	security-control/RDS.4
aws-foundational-security-best-Práticas/V/1.0.0/RDS.5	security-control/RDS.5
aws-foundational-security-best-Práticas/V/1.0.0/RDS.6	security-control/RDS.6
aws-foundational-security-best-Práticas/V/1.0.0/RDS.7	security-control/RDS.7
aws-foundational-security-best-Práticas/V/1.0.0/RDS.8	security-control/RDS.8
aws-foundational-security-best-Práticas/V/1.0.0/RDS.9	security-control/RDS.9
aws-foundational-security-best-Práticas/V/1.0.0/Redshift.1	security-control/Redshift.1

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
aws-foundational-security-best- Práticas/V/1.0.0/Redshift.2	security-control/Redshift.2
aws-foundational-security-best-Práticas/V/1.0.0/Redshift.3	security-control/Redshift.3
aws-foundational-security-best- Práticas/V/1.0.0/Redshift.4	security-control/Redshift.4
aws-foundational-security-best-Práticas/V/1.0.0/Redshift.6	security-control/Redshift.6
aws-foundational-security-best-Práticas/V/1.0.0/Redshift.7	security-control/Redshift.7
aws-foundational-security-best-Práticas/V/1.0.0/Redshift.8	security-control/Redshift.8
aws-foundational-security-best-Práticas/V/1.0.0/Redshift.9	security-control/Redshift.9
aws-foundational-security-best-Práticas/V/1.0.0/S3.1	security-control/S3.1
aws-foundational-security-best-Práticas/V/1.0.0/S3.12	security-control/S3.12
aws-foundational-security-best-Práticas/V/1.0.0/S3.13	security-control/S3.12
aws-foundational-security-best-Práticas/V/1.0.0/S3.2	security-control/S3.2
aws-foundational-security-best-Práticas/V/1.0.0/S3.3	security-control/S3.3

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
aws-foundational-security-best-Práticas/V/1.0.0/S3.5	security-control/S3.5
aws-foundational-security-best-Práticas/V/1.0.0/S3.6	security-control/S3.6
aws-foundational-security-best-Práticas/V/1.0.0/S3.8	security-control/S3.8
aws-foundational-security-best-Práticas/V/1.0.0/S3.9	security-control/S3.9
aws-foundational-security-best-práticas/v/1.0.0/ .1 SageMaker	controle de segurança/ 1SageMaker.
aws-foundational-security-best-práticas/v/1.0.0/ .2 SageMaker	controle de segurança/ 2SageMaker.
aws-foundational-security-best-práticas/v/1.0.0/ .3 SageMaker	controle de segurança/ 3SageMaker.
aws-foundational-security-best-práticas/v/1.0.0/ .1 SecretsManager	controle de segurança/ 1SecretsManager.
aws-foundational-security-best-práticas/v/1.0.0/ .2 SecretsManager	controle de segurança/ 2SecretsManager.
aws-foundational-security-best-práticas/v/1.0.0/ .3 SecretsManager	controle de segurança/ 3SecretsManager.
aws-foundational-security-best-práticas/v/1.0.0/ 1.4 SecretsManager	controle de segurança/ 4SecretsManager.
aws-foundational-security-best-Práticas/V/1.0.0/SQS.1	security-control/SQS.1

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
aws-foundational-security-best-Práticas/V/1.0.0/SSM.1	security-control/SSM.1
aws-foundational-security-best-Práticas/V/1.0.0/SSm.2	security-control/SSM.2
aws-foundational-security-best-Práticas/V/1.0.0/SSm.3	security-control/SSM.3
aws-foundational-security-best-Práticas/V/1.0.0/SSm.4	security-control/SSM.4
aws-foundational-security-best-Práticas/V/1.0.0/WAF.1	security-control/WAF.1
aws-foundational-security-best-Práticas/V/1.0.0/WAF.2	security-control/WAF.2
aws-foundational-security-best-Práticas/V/1.0.0/WAF.3	security-control/WAF.3
aws-foundational-security-best-Práticas/V/1.0.0/WAF.4	security-control/WAF.4
aws-foundational-security-best-Práticas/V/1.0.0/WAF.6	security-control/WAF.6
aws-foundational-security-best-Práticas/V/1.0.0/WAF.7	security-control/WAF.7
aws-foundational-security-best-Práticas/V/1.0.0/WAF.8	security-control/WAF.8
aws-foundational-security-best-Práticas/V/1.0.0/WAF.10	security-control/WAF.10
PCI-DSS/V/3.2.1/PCI. AutoScaling.1	controle de segurança/ 1AutoScaling.

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
PCI-DSS/V/3.2.1/PCI. CloudTrail.1	controle de segurança/ 2CloudTrail.
PCI-DSS/V/3.2.1/PCI. CloudTrail.2	controle de segurança/ 3CloudTrail.
PCI-DSS/V/3.2.1/PCI. CloudTrail.3	controle de segurança/ 4CloudTrail.
PCI-DSS/V/3.2.1/PCI. CloudTrail.4	controle de segurança/ 5CloudTrail.
PCI-DSS/V/3.2.1/PCI. CodeBuild.1	controle de segurança/ 1CodeBuild.
PCI-DSS/V/3.2.1/PCI. CodeBuild.2	controle de segurança/ 2CodeBuild.
pci-dss/v/3.2.1/PCI.Config.1	security-control/Config.1
pci-dss/v/3.2.1/PCI.CW.1	controle de segurança/ 1CloudWatch.
pci-dss/v/3.2.1/PCI.DMS.1	security-control/DMS.1
pci-dss/v/3.2.1/PCI.EC2.1	security-control/EC2.1
pci-dss/v/3.2.1/PCI.EC2.2	security-control/EC2.2
pci-dss/v/3.2.1/PCI.EC2.4	security-control/EC2.12
pci-dss/v/3.2.1/PCI.EC2.5	security-control/EC2.13
pci-dss/v/3.2.1/PCI.EC2.6	security-control/EC2.6
pci-dss/v/3.2.1/PCI.ELBv2.1	security-control/ELB.1
pci-dss/v/3.2.1/PCI.ES.1	security-control/ES.2
pci-dss/v/3.2.1/PCI.ES.2	security-control/ES.1
PCI-DSS/V/3.2.1/PCI. GuardDuty.1	controle de segurança/ 1GuardDuty.
pci-dss/v/3.2.1/PCI.IAM.1	security-control/IAM.4
pci-dss/v/3.2.1/PCI.IAM.2	security-control/IAM.2

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
pci-dss/v/3.2.1/PCI.IAM.3	security-control/IAM.1
pci-dss/v/3.2.1/PCI.IAM.4	security-control/IAM.6
pci-dss/v/3.2.1/PCI.IAM.5	security-control/IAM.9
pci-dss/v/3.2.1/PCI.IAM.6	security-control/IAM.19
pci-dss/v/3.2.1/PCI.IAM.7	security-control/IAM.8
pci-dss/v/3.2.1/PCI.IAM.8	security-control/IAM.10
pci-dss/v/3.2.1/PCI.KMS.1	security-control/KMS.4
pci-dss/v/3.2.1/PCI.Lambda.1	security-control/Lambda.1
pci-dss/v/3.2.1/PCI.Lambda.2	security-control/Lambda.3
pci-dss/v/3.2.1/PCI.Opensearch.1	security-control/Opensearch.2
pci-dss/v/3.2.1/PCI.Opensearch.2	security-control/Opensearch.1
pci-dss/v/3.2.1/PCI.RDS.1	security-control/RDS.1
pci-dss/v/3.2.1/PCI.RDS.2	security-control/RDS.3
pci-dss/v/3.2.1/PCI.Redshift.1	security-control/Redshift.1
pci-dss/v/3.2.1/PCI.S3.1	security-control/S3.3
pci-dss/v/3.2.1/PCI.S3.2	security-control/S3.2
pci-dss/v/3.2.1/PCI.S3.3	security-control/S3.7
pci-dss/v/3.2.1/PCI.S3.5	security-control/S3.5
pci-dss/v/3.2.1/PCI.S3.5	security-control/S3.1
PCI-DSS/V/3.2.1/PCI. SageMaker.1	controle de segurança/ 1SageMaker.

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
pci-dss/v/3.2.1/PCI.SSM.1	security-control/SSM.2
pci-dss/v/3.2.1/PCI.SSM.2	security-control/SSM.3
pci-dss/v/3.2.1/PCI.SSM.3	security-control/SSM.1
service-managed-aws-control-Torre/V/1.0.0/ ACM.1	security-control/ACM.1
service-managed-aws-control- Torre/V/1.0.0/ API Gateway.1	security-control/APIGateway.1
service-managed-aws-control- Torre/V/1.0.0/ API Gateway.2	security-control/APIGateway.2
service-managed-aws-control- Torre/V/1.0.0/ API Gateway.3	security-control/APIGateway.3
service-managed-aws-control- Torre/V/1.0.0/ API Gateway.4	security-control/APIGateway.4
service-managed-aws-control- Torre/V/1.0.0/ API Gateway.5	security-control/APIGateway.5
service-managed-aws-controlAutoScaling-torre/ v/1.0.0/ .1	controle de segurança/ 1AutoScaling.
service-managed-aws-controlAutoScaling-torre/ v/1.0.0/ 1.2	controle de segurança/ 2AutoScaling.
service-managed-aws-controlAutoScaling-torre/ v/1.0.0/ .3	controle de segurança/ 3AutoScaling.
service-managed-aws-controlAutoScaling-torre/ v/1.0.0/ 1.4	controle de segurança/ 4AutoScaling.

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
service-managed-aws-control-Torre/V/1.0.0/escalabilidade automática.5	security-control/Autoscaling.5
service-managed-aws-controlAutoScaling-torre/v/1.0.0/ 6.0	controle de segurança/ 6AutoScaling.
service-managed-aws-controlAutoScaling-torre/v/1.0.0/ 9.0	controle de segurança/ 9AutoScaling.
service-managed-aws-controlCloudTrail-torre/v/1.0.0/ .1	controle de segurança/ 1CloudTrail.
service-managed-aws-controlCloudTrail-torre/v/1.0.0/ 1.2	controle de segurança/ 2CloudTrail.
service-managed-aws-controlCloudTrail-torre/v/1.0.0/ 1.4	controle de segurança/ 4CloudTrail.
service-managed-aws-controlCloudTrail-torre/v/1.0.0/ 0,5	controle de segurança/ 5CloudTrail.
service-managed-aws-controlCodeBuild-torre/v/1.0.0/ .1	controle de segurança/ 1CodeBuild.
service-managed-aws-controlCodeBuild-torre/v/1.0.0/ 1.2	controle de segurança/ 2CodeBuild.
service-managed-aws-controlCodeBuild-torre/v/1.0.0/ 1.4	controle de segurança/ 4CodeBuild.
service-managed-aws-controlCodeBuild-torre/v/1.0.0/ 0,5	controle de segurança/ 5CodeBuild.
service-managed-aws-control-Torre/V/1.0.0/DMS.1	security-control/DMS.1

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
service-managed-aws-control-Torre/V/1.0.0/DynamoDB.1	security-control/DynamoDB.1
service-managed-aws-control-Torre/V/1.0.0/DynamoDB.2	security-control/DynamoDB.2
service-managed-aws-control-Torre/V/1.0.0/EC2.1	security-control/EC2.1
service-managed-aws-control-Torre/V/1.0.0/EC2.2	security-control/EC2.2
service-managed-aws-control-Torre/V/1.0.0/EC2.3	security-control/EC2.3
service-managed-aws-control-Torre/V/1.0.0/EC2.4	security-control/EC2.4
service-managed-aws-control-Torre/V/1.0.0/EC2.6	security-control/EC2.6
service-managed-aws-control-Torre/V/1.0.0/EC2.7	security-control/EC2.7
service-managed-aws-control-Torre/V/1.0.0/EC2.8	security-control/EC2.8
service-managed-aws-control-Torre/V/1.0.0/EC2.9	security-control/EC2.9
service-managed-aws-control-Torre/V/1.0.0/EC2.10	security-control/EC2.10
service-managed-aws-control-Torre/V/1.0.0/EC2.15	security-control/EC2.15

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
service-managed-aws-control-Torre/V/1.0.0/EC2.16	security-control/EC2.16
service-managed-aws-control-Torre/V/1.0.0/EC2.17	security-control/EC2.17
service-managed-aws-control-Torre/V/1.0.0/EC2.18	security-control/EC2.18
service-managed-aws-control-Torre/V/1.0.0/EC2.19	security-control/EC2.19
service-managed-aws-control-Torre/V/1.0.0/EC2.20	security-control/EC2.20
service-managed-aws-control-Torre/V/1.0.0/EC2.21	security-control/EC2.21
service-managed-aws-control-Torre/V/1.0.0/EC2.22	security-control/EC2.22
service-managed-aws-control-Torre/V/1.0.0/ECr.1	security-control/ECR.1
service-managed-aws-control-Torre/V/1.0.0/ECR.2	security-control/ECR.2
service-managed-aws-control-Torre/V/1.0.0/ECr.3	security-control/ECR.3
service-managed-aws-control-Torre/V/1.0.0/ECS.1	security-control/ECS.1
service-managed-aws-control-Torre/V/1.0.0/ECS.2	security-control/ECS.2

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
service-managed-aws-control-Torre/V/1.0.0/ECS.3	security-control/ECS.3
service-managed-aws-control-Torre/V/1.0.0/ECS.4	security-control/ECS.4
service-managed-aws-control-Torre/V/1.0.0/ECS.5	security-control/ECS.5
service-managed-aws-control-Torre/V/1.0.0/ECS.8	security-control/ECS.8
service-managed-aws-control-Torre/V/1.0.0/ECS.10	security-control/ECS.10
service-managed-aws-control-Torre/V/1.0.0/ECS.12	security-control/ECS.12
service-managed-aws-control-Torre/V/1.0.0/EFS.1	security-control/EFS.1
service-managed-aws-control-Torre/V/1.0.0/EFS.2	security-control/EFS.2
service-managed-aws-control-Torre/V/1.0.0/EFS.3	security-control/EFS.3
service-managed-aws-control-Torre/V/1.0.0/EFS.4	security-control/EFS.4
service-managed-aws-control-Torre/V/1.0.0/EKS.2	security-control/EKS.2
service-managed-aws-control-Torre/V/1.0.0/ELB.2	security-control/ELB.2

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
service-managed-aws-control-Torre/V/1.0.0/ELB.3	security-control/ELB./*
service-managed-aws-control-Torre/V/1.0.0/ELB.4	security-control/ELB.4
service-managed-aws-control-Torre/V/1.0.0/ELB.5	security-control/ELB.5
service-managed-aws-control-Torre/V/1.0.0/ELB.6	security-control/ELB.6
service-managed-aws-control-Torre/V/1.0.0/ELB.7	security-control/ELB.7
service-managed-aws-control-Torre/V/1.0.0/ELB.8	security-control/ELB.8
service-managed-aws-control-Torre/V/1.0.0/ELB.9	security-control/ELB.9
service-managed-aws-control-Torre/V/1.0.0/ELB.10	security-control/ELB.10
service-managed-aws-control-Torre/V/1.0.0/ELB.12	security-control/ELB.12
service-managed-aws-control-Torre/V/1.0.0/ELB.13	security-control/ELB.13
service-managed-aws-control-Torre/V/1.0.0/ELB.14	security-control/ELB.14
service-managed-aws-control-Torre/V/1.0.0/ELBV2.1	security-control/ELBv2.1

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
service-managed-aws-control-Torre/V/1.0.0/EMR.1	security-control/EMR.1
service-managed-aws-control-Torre/V/1.0.0/ES.1	security-control/ES.1
service-managed-aws-control-Torre/V/1.0.0/ES.2	security-control/ES.2
service-managed-aws-control-Torre/V/1.0.0/ES.3	security-control/ES.3
service-managed-aws-control-Torre/V/1.0.0/ES.4	security-control/ES.4
service-managed-aws-control-Torre/V/1.0.0/ES.5	security-control/ES.5
service-managed-aws-control-Torre/V/1.0.0/ES.6	security-control/ES.6
service-managed-aws-control-Torre/V/1.0.0/ES.7	security-control/ES.7
service-managed-aws-control-Torre/V/1.0.0/ES.8	security-control/ES.8
service-managed-aws-controlElasticBeanstalk-torre/v/1.0.0/ .1	controle de segurança/ 1ElasticBeanstalk.
service-managed-aws-controlElasticBeanstalk-torre/v/1.0.0/ 1.2	controle de segurança/ 2ElasticBeanstalk.
service-managed-aws-controlGuardDuty-torre/v/1.0.0/ .1	controle de segurança/ 1GuardDuty.

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
service-managed-aws-control-Torre/V/1.0.0/IAM.1	security-control/IAM.1
service-managed-aws-control-Torre/V/1.0.0/IAM.2	security-control/IAM.2
service-managed-aws-control-Torre/V/1.0.0/IAM.3	security-control/IAM.3
service-managed-aws-control-Torre/V/1.0.0/IAM.4	security-control/IAM.4
service-managed-aws-control-Torre/V/1.0.0/IAM.5	security-control/IAM.5
service-managed-aws-control-Torre/V/1.0.0/IAM.6	security-control/IAM.6
service-managed-aws-control-Torre/V/1.0.0/IAM.7	security-control/IAM.7
service-managed-aws-control-Torre/V/1.0.0/IAM.8	security-control/IAM.8
service-managed-aws-control-Torre/V/1.0.0/IAM.21	security-control/IAM.21
service-managed-aws-control-Torre/V/1.0.0/Kinesis.1	security-control/Kinesis.1
service-managed-aws-control-Torre/V/1.0.0/kms.1	security-control/KMS.1
service-managed-aws-control-Torre/V/1.0.0/kms.2	security-control/KMS.2

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
service-managed-aws-control-Torre/V/1.0.0/km.3	security-control/KMS.3
service-managed-aws-control-Torre/V/1.0.0/Lambda.1	security-control/Lambda.1
service-managed-aws-control-Torre/V/1.0.0/Lambda.2	security-control/Lambda.2
service-managed-aws-control-Torre/V/1.0.0/Lambda.5	security-control/Lambda.5
service-managed-aws-controlNetworkFirewall-torre/v/1.0.0/ .3	controle de segurança/ 3NetworkFirewall.
service-managed-aws-controlNetworkFirewall-torre/v/1.0.0/ 1.4	controle de segurança/ 4NetworkFirewall.
service-managed-aws-controlNetworkFirewall-torre/v/1.0.0/ 0,5	controle de segurança/ 5NetworkFirewall.
service-managed-aws-controlNetworkFirewall-torre/v/1.0.0/ 6.0	controle de segurança/ 6NetworkFirewall.
service-managed-aws-control- Torre/V/1.0.0/OpenSearch.1	security-control/Opensearch.1
service-managed-aws-control- Torre/V/1.0.0/OpenSearch.2	security-control/Opensearch.2
service-managed-aws-control- Torre/V/1.0.0/OpenSearch.3	security-control/Opensearch.3
service-managed-aws-control- Torre/V/1.0.0/OpenSearch.4	security-control/Opensearch.4

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
service-managed-aws-control- Torre/V/1.0.0/ OpenSearch.5	security-control/Opensearch.5
service-managed-aws-control- Torre/V/1.0.0/ OpenSearch.6	security-control/Opensearch.6
service-managed-aws-control- Torre/V/1.0.0/ OpenSearch.7	security-control/Opensearch.7
service-managed-aws-control- Torre/V/1.0.0/ OpenSearch.8	security-control/Opensearch.8
service-managed-aws-control-Torre/V/1.0.0/ RDS.1	security-control/RDS.1
service-managed-aws-control-Torre/V/1.0.0/ RDS.2	security-control/RDS.3
service-managed-aws-control-Torre/V/1.0.0/ RDS.3	security-control/RDS.3
service-managed-aws-control-Torre/V/1.0.0/ RDS.4	security-control/RDS.4
service-managed-aws-control-Torre/V/1.0.0/ RDS.5	security-control/RDS.5
service-managed-aws-control-Torre/V/1.0.0/ RDS.6	security-control/RDS.6
service-managed-aws-control-Torre/V/1.0.0/ RDS.8	security-control/RDS.8
service-managed-aws-control-Torre/V/1.0.0/ RDS.9	security-control/RDS.9

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
service-managed-aws-control-Torre/V/1.0.0/RDS.10	security-control/RDS.10
service-managed-aws-control-Torre/V/1.0.0/RDS.11	security-control/RDS.11
service-managed-aws-control-Torre/V/1.0.0/RDS.13	security-control/RDS.13
service-managed-aws-control-Torre/V/1.0.0/RDS.17	security-control/RDS.17
service-managed-aws-control-Torre/V/1.0.0/RDS.18	security-control/RDS.18
service-managed-aws-control-Torre/V/1.0.0/RDS.19	security-control/RDS.19
service-managed-aws-control-Torre/V/1.0.0/RDS.20	security-control/RDS.20
service-managed-aws-control-Torre/V/1.0.0/RDS.21	security-control/RDS.21
service-managed-aws-control-Torre/V/1.0.0/RDS.22	security-control/RDS.22
service-managed-aws-control-Torre/V/1.0.0/RDS.23	security-control/RDS.23
service-managed-aws-control-Torre/V/1.0.0/RDS.25	security-control/RDS.25
service-managed-aws-control-Torre/V/1.0.0/Redshift.1	security-control/Redshift.1

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
service-managed-aws-control-Torre/V/1.0.0/Redshift.2	security-control/Redshift.2
service-managed-aws-control-Torre/V/1.0.0/Redshift.4	security-control/Redshift.4
service-managed-aws-control-Torre/V/1.0.0/Redshift.6	security-control/Redshift.6
service-managed-aws-control-Torre/V/1.0.0/Redshift.7	security-control/Redshift.7
service-managed-aws-control-Torre/V/1.0.0/Redshift.8	security-control/Redshift.8
service-managed-aws-control-Torre/V/1.0.0/Redshift.9	security-control/Redshift.9
service-managed-aws-control-Torre/V/1.0.0/S3.1	security-control/S3.1
service-managed-aws-control-Torre/V/1.0.0/S3.2	security-control/S3.2
service-managed-aws-control-Torre/V/1.0.0/S3.3	security-control/S3.3
service-managed-aws-control-Torre/V/1.0.0/S3.5	security-control/S3.5
service-managed-aws-control-Torre/V/1.0.0/S3.6	security-control/S3.6
service-managed-aws-control-Torre/V/1.0.0/S3.8	security-control/S3.8

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
service-managed-aws-control-Torre/V/1.0.0/S3.9	security-control/S3.9
service-managed-aws-control-Torre/V/1.0.0/S3.12	security-control/S3.12
service-managed-aws-control-Torre/V/1.0.0/S3.13	security-control/S3.12
service-managed-aws-controlSageMaker-torre/v/1.0.0/ .1	controle de segurança/ 1SageMaker.
service-managed-aws-controlSecretsManager-torre/v/1.0.0/ .1	controle de segurança/ 1SecretsManager.
service-managed-aws-controlSecretsManager-torre/v/1.0.0/ 1.2	controle de segurança/ 2SecretsManager.
service-managed-aws-controlSecretsManager-torre/v/1.0.0/ .3	controle de segurança/ 3SecretsManager.
service-managed-aws-controlSecretsManager-torre/v/1.0.0/ 1.4	controle de segurança/ 4SecretsManager.
service-managed-aws-control-Torre/V/1.0.0/SQS.1	security-control/SQS.1
service-managed-aws-control-Torre/V/1.0.0/SSm.1	security-control/SSM.1
service-managed-aws-control-Torre/V/1.0.0/SSm.2	security-control/SSM.2
service-managed-aws-control-Torre/V/1.0.0/SSm.3	security-control/SSM.3

GeneratorID antes de ativar as descobertas de controle consolidadas	GeneratorID depois de ativar as descobertas de controle consolidadas
service-managed-aws-control-Torre/V/1.0.0/SSm.4	security-control/SSM.4
service-managed-aws-control-Torre/V/1.0.0/Waf.2	security-control/WAF.2
service-managed-aws-control-Torre/V/1.0.0/Waf.3	security-control/WAF.3
service-managed-aws-control-Torre/V/1.0.0/Waf.4	security-control/WAF.4

Como a consolidação afeta os IDs e títulos de controle

A visualização de controles consolidados e as descobertas de controle consolidadas padronizam IDs e títulos de controle em todos os padrões. Os termos ID de controle de segurança e título de controle de segurança se referem a esses valores independentes de padrão. A tabela a seguir mostra o mapeamento de IDs e títulos de controle de segurança para IDs e títulos de controle específicos do padrão. IDs e títulos para controles que pertencem ao padrão AWS Foundational Security Best Practices (FSBP) inalterados.

O console do Security Hub exibe IDs de controle de segurança e títulos de controle de segurança, independentemente de as descobertas de controle consolidadas estarem ativadas ou desativadas em sua conta. Entretanto, as descobertas do Security Hub contêm IDs de controle de segurança e títulos somente se as descobertas de controle consolidadas estiverem ativadas na sua conta. Se as descobertas de controle consolidadas estiverem desativadas em sua conta, as descobertas do Security Hub conterão IDs e títulos de controle específicos do padrão. Para obter mais informações sobre como a consolidação afeta as descobertas de controle, consulte Exemplo de descobertas de controle.

Para controles que fazem parte do Service-Managed Standard: AWS Control Tower, o prefixo `CT.` é removido da ID de controle e do título nas descobertas quando as descobertas de controle consolidadas são ativadas.

Para executar seus próprios scripts nessa tabela, baixe-a como um arquivo.csv.

Padrão	ID e título do controle padrão	ID e título do controle de segurança
CIS v1.2.0	1.1 Evitar o uso do "usuário raiz"	[CloudWatch.1] Um filtro métrico de log e um alarme devem existir para uso do usuário “root”
CIS v1.2.0	1.10 Certifique-se de que a política de senha do IAM impeça a reutilização de senhas	1.10 Certifique-se de que a política de senha do IAM impeça a reutilização de senhas
CIS v1.2.0	1.11 Certifique-se de que a política de senha do IAM expire senhas em até 90 dias ou menos	1.11 Certifique-se de que a política de senha do IAM expire senhas em até 90 dias ou menos
CIS v1.2.0	1.12 Certifique-se que não existam chaves de acesso do usuário raiz	[IAM.4] A chave de acesso do usuário raiz do não deve existir
CIS v1.2.0	1.13 Certifique-se que MFA esteja habilitada para a usuário raiz	[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
CIS v1.2.0	1.14 Certifique-se que a MFA de hardware esteja habilitada para o usuário raiz	[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
CIS v1.2.0	1.16 Certifique-se que as políticas do IAM sejam anexadas somente a grupos ou funções	[IAM.2] Os usuários do não devem ter políticas do IAM anexadas
CIS v1.2.0	1.2 Certifique-se de que a autenticação multifator (MFA) esteja ativada para todos os usuários do IAM que têm uma senha do console	[IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console
CIS v1.2.0	1.20 Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support	[IAM.18] Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support

Padrão	ID e título do controle padrão	ID e título do controle de segurança
CIS v1.2.0	1.22 Certifique-se que as políticas do IAM que permitem privilégios administrativos "*:*" completos não sejam criadas	[IAM.1] As políticas do não devem permitir privilégios administrativos completos "*"
CIS v1.2.0	1.3 Certifique-se de que as credencia is não usadas por 90 dias ou mais sejam desativadas	As credenciais de usuário do IAM não utilizadas devem ser removidas
CIS v1.2.0	1.4 Certifique-se de que as chaves de acesso sejam mudadas a cada 90 dias ou menos	[IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos
CIS v1.2.0	1.5 Certifique-se que política de senha do IAM exija pelo menos uma letra maiúscula	1.5 Certifique-se de que política de senha do IAM exija pelo menos uma letra maiúscula
CIS v1.2.0	1.6 Certifique-se que a política de senha do IAM exija pelo menos uma letra minúscula	1.6 Certifique-se de que política de senha do IAM exija pelo menos uma letra minúscula
CIS v1.2.0	1.7 Certifique-se de que política de senha do IAM exija pelo menos um símbolo	1.7 Certifique-se de que política de senha do IAM exija pelo menos um símbolo
CIS v1.2.0	Certifique-se que a política de senha do IAM exija pelo menos um número	Certifique-se de que política de senha do IAM exija pelo menos um número
CIS v1.2.0	1.9 Certifique-se que a política de senha do IAM exija um comprimento mínimo de 14 ou mais	1.9 Certifique-se de que a política de senha do IAM exija um comprimento mínimo de 14 ou mais

Padrão	ID e título do controle padrão	ID e título do controle de segurança
CIS v1.2.0	2.1 Certifique-se de que CloudTrail está ativado em todas as regiões	[CloudTrail.1] CloudTrail deve ser habilitado e configurado com pelo menos uma trilha multirregional que inclua eventos de gerenciamento de leitura e gravação
CIS v1.2.0	2.2 Certifique-se de que a validação do arquivo de CloudTrail log esteja ativada	[CloudTrail.4] a validação do arquivo de CloudTrail log deve estar ativada
CIS v1.2.0	2.3 Certifique-se de que o bucket do S3 usado para armazenar CloudTrai l registros não esteja acessível ao público	[CloudTrail.6] Certifique-se de que o bucket do S3 usado para armazenar CloudTrail registros não esteja acessível ao público
CIS v1.2.0	2.4 Garanta que as CloudTrail trilhas estejam integradas aos CloudWatch registros	[CloudTrail.5] CloudTrail trilhas devem ser integradas com o Amazon CloudWatch Logs
CIS v1.2.0	2.5 Certifique-se de que AWS Config está ativado	[Config.1] AWS Config deve estar habilitado
CIS v1.2.0	2.6 Certifique-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrail S3	[CloudTrail.7] Certifique-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrail S3
CIS v1.2.0	2.7 Certifique-se de que CloudTrail os registros sejam criptografados em repouso usando CMKs do KMS	[CloudTrail.2] CloudTrail deve ter a criptografia em repouso ativada
CIS v1.2.0	2.8 Verifique se a rotação para CMKs criadas pelo cliente está habilitada	A rotação de AWS KMS teclas [KMS.4] deve estar ativada
CIS v1.2.0	2.9 Verifique se o registro de fluxo da VPC está ativado em todas as VPCs	[EC2.6] O registro de fluxo de VPC deve ser ativado em todas as VPCs

Padrão	ID e título do controle padrão	ID e título do controle de segurança
CIS v1.2.0	3.1 Certifique-se de que um filtro e um alarme de métrica de logs existam para chamadas de API não autorizadas	[CloudWatch.2] Certifique-se de que exista um filtro métrico de registro e um alarme para chamadas de API não autorizadas
CIS v1.2.0	3.10 Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de grupo de segurança	[CloudWatch.10] Certifique-se de que exista um filtro métrico de log e um alarme para alterações no grupo de segurança
CIS v1.2.0	3.11 Garanta que um filtro e um alarme de métrica de logs existem para alterações em listas de controle de acesso à rede (NACL)	[CloudWatch.11] Certifique-se de que exista um filtro métrico de registro e um alarme para alterações nas listas de controle de acesso à rede (NACL)
CIS v1.2.0	3.12 Garanta que um filtro e um alarme de métrica de logs existem para alterações em gateways de rede	[CloudWatch.12] Certifique-se de que exista um filtro métrico de log e um alarme para alterações nos gateways de rede
CIS v1.2.0	3.13 Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de tabela de rotas	[CloudWatch.13] Certifique-se de que exista um filtro métrico de log e um alarme para alterações na tabela de rotas
CIS v1.2.0	3.14 Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de VPC	[CloudWatch.14] Certifique-se de que exista um filtro métrico de log e um alarme para alterações de VPC
CIS v1.2.0	3.2 Certifique-se que um filtro e um alarme de métrica de logs existam para login do Management Console sem a MFA	[CloudWatch.3] Certifique-se de que exista um filtro métrico de registro e um alarme para o login do Management Console sem MFA

Padrão	ID e título do controle padrão	ID e título do controle de segurança
CIS v1.2.0	3.3 Certifique-se que um filtro e um alarme de métrica de logs existam para uso do usuário raiz	[CloudWatch.1] Um filtro métrico de log e um alarme devem existir para uso do usuário “root”
CIS v1.2.0	3.4 Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de política do IAM	[CloudWatch.4] Certifique-se de que exista um filtro de métrica de log e um alarme para alterações na política do IAM
CIS v1.2.0	3.5 Certifique-se de que exista um filtro métrico de registro e um alarme para alterações CloudTrail de configuração	[CloudWatch.5] Certifique-se de que exista um filtro métrico de log e um alarme para alterações de CloudTrail AWS Config duração
CIS v1.2.0	3.6 Certifique-se de que exista um filtro métrico de registro e um alarme para falhas de AWS Management Console autenticação	[CloudWatch.6] Certifique-se de que exista um filtro métrico de registro e um alarme para falhas de AWS Management Console autenticação
CIS v1.2.0	3.7 Certifique-se de que exita um filtro e um alarme de métrica de logs para a desativação ou exclusão programada de CMKs criadas pelo cliente	[CloudWatch.7] Certifique-se de que exista um filtro métrico de registro e um alarme para desativar ou excluir programadamente as chaves gerenciadas pelo cliente
CIS v1.2.0	3.8 Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de política de bucket do S3	[CloudWatch.8] Certifique-se de que exista um filtro métrico de log e um alarme para alterações na política do bucket do S3
CIS v1.2.0	3.9 Certifique-se de que exista um filtro métrico de log e um alarme para alterações AWS Config de configura ção	[CloudWatch.9] Certifique-se de que exista um filtro métrico de registro e um alarme para alterações AWS Config de configuração

Padrão	ID e título do controle padrão	ID e título do controle de segurança
CIS v1.2.0	4.1 Certifique-se de nenhum grupo de segurança permita a entrada de 0.0.0.0/0 na porta 22	[EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22
CIS v1.2.0	4.2 Certifique-se de nenhum grupo de segurança permita a entrada de 0.0.0.0/0 na porta 3389	[EC2.14] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 3389
CIS v1.2.0	4.3 Verifique se o grupo de segurança padrão de cada VPC restringe todo o tráfego	[EC2.2] O grupo de segurança padrão da VPC não deve permitir o tráfego de entrada e saída
CIS v1.4.0	1.10 Certifique-se de que a autentica ção multifator (MFA) esteja ativada para todos os usuários do IAM que têm uma senha do console	[IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console
CIS v1.4.0	1.4 Certifique-se de que as chaves de acesso sejam mudadas a cada 90 dias ou menos	[IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos
CIS v1.4.0	1.16 Certifique-se que as políticas do IAM que permitem privilégios administrativos "*:*" completos não sejam A	[IAM.1] As políticas do não devem permitir privilégios administrativos completos "*"
CIS v1.4.0	1.17 Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support	[IAM.18] Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support
CIS v1.4.0	1.4 Certifique-se de que não existam chaves de acesso da conta raiz	[IAM.4] A chave de acesso do usuário raiz do não deve existir
CIS v1.4.0	1.5 Certifique-se que A MFA esteja habilitada para a conta do usuário raiz	[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz

Padrão	ID e título do controle padrão	ID e título do controle de segurança
CIS v1.4.0	1.14 Certifique-se que a MFA de hardware esteja habilitada para a conta de usuário raiz	[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
CIS v1.4.0	1.7 Elimine o uso do usuário raiz para tarefas administrativas e diárias	[CloudWatch.1] Um filtro métrico de log e um alarme devem existir para uso do usuário “root”
CIS v1.4.0	1.8 Certifique-se que a política de senha do IAM exija um comprimento mínimo de 14 ou mais	1.9 Certifique-se de que a política de senha do IAM exija um comprimento mínimo de 14 ou mais
CIS v1.4.0	1.9 Certifique-se que a política de senha do IAM impeça a reutilização de senhas	1.10 Certifique-se de que a política de senha do IAM impeça a reutilização de senhas
CIS v1.4.0	2.1.2 Certifique-se que a política de bucket do S3 esteja configurada para negar solicitações HTTP	[S3.5] Os buckets de uso geral do S3 devem exigir solicitações de uso de SSL
CIS v1.4.0	2.1.5.1 A configuração do S3 Block Public Access deve estar habilitada	[S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas
CIS v1.4.0	2.1.5.2 A configuração de acesso público do bloco S3 deve ser ativada no nível do bucket	[S3.8] Os buckets de uso geral do S3 devem bloquear o acesso público
CIS v1.4.0	2.2.1 Certifique-se que a criptografia de volume do EBS esteja ativada	[EC2.7] A criptografia padrão do EBS deve estar ativada
CIS v1.4.0	2.3.1 Certifique-se de que a criptografia esteja habilitada para instâncias do RDS	[RDS.3] As instâncias de banco de dados do RDS devem ter a criptografia em repouso habilitada.

Padrão	ID e título do controle padrão	ID e título do controle de segurança
CIS v1.4.0	3.1 Certifique-se de que CloudTrail está habilitado em todas as regiões	[CloudTrail.1] CloudTrail deve ser habilitado e configurado com pelo menos uma trilha multirregional que inclua eventos de gerenciamento de leitura e gravação
CIS v1.4.0	3.2 Certifique-se de que a validação do arquivo de CloudTrail log esteja ativada	[CloudTrail.4] a validação do arquivo de CloudTrail log deve estar ativada
CIS v1.4.0	3.4 Garanta que as CloudTrail trilhas estejam integradas aos registros CloudWatch	[CloudTrail.5] CloudTrail trilhas devem ser integradas com o Amazon CloudWatch Logs
CIS v1.4.0	3.5 Certifique-se de que AWS Config está habilitado em todas as regiões	[Config.1] AWS Config deve estar habilitado
CIS v1.4.0	3.6 Certifique-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrail S3	[CloudTrail.7] Certifique-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrail S3
CIS v1.4.0	3.7 Certifique-se de que CloudTrail os registros sejam criptografados em repouso usando CMKs do KMS	[CloudTrail.2] CloudTrail deve ter a criptografia em repouso ativada
CIS v1.4.0	3.8 Verifique se a alternância para CMKs criadas pelo cliente está habilitada	A rotação de AWS KMS teclas [KMS.4] deve estar ativada
CIS v1.4.0	3.9 Verifique se o registro de fluxo da VPC está ativado em todas as VPCs	[EC2.6] O registro de fluxo de VPC deve ser ativado em todas as VPCs
CIS v1.4.0	4.4 Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de política do IAM	[CloudWatch.4] Certifique-se de que exista um filtro de métrica de log e um alarme para alterações na política do IAM

Padrão	ID e título do controle padrão	ID e título do controle de segurança
CIS v1.4.0	4.5 Certifique-se de que exista um filtro métrico de log e um alarme para alterações CloudTrail de configura ção	[CloudWatch.5] Certifique-se de que exista um filtro métrico de log e um alarme para alterações de CloudTrail AWS Config duração
CIS v1.4.0	4.6 Certifique-se de que exista um filtro métrico de registro e um alarme para falhas de AWS Management Console autenticação	[CloudWatch.6] Certifique-se de que exista um filtro métrico de registro e um alarme para falhas de AWS Management Console autenticação
CIS v1.4.0	4.7 Certifique-se de que exita um filtro e um alarme de métrica de logs para a desativação ou exclusão programada de CMKs criadas pelo cliente	[CloudWatch.7] Certifique-se de que exista um filtro métrico de registro e um alarme para desativar ou excluir programadamente as chaves gerenciadas pelo cliente
CIS v1.4.0	4.8 Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de política de bucket do S3	[CloudWatch.8] Certifique-se de que exista um filtro métrico de log e um alarme para alterações na política do bucket do S3
CIS v1.4.0	4.9 Certifique-se de que exista um filtro métrico de log e um alarme para alterações AWS Config de configura ção	[CloudWatch.9] Certifique-se de que exista um filtro métrico de registro e um alarme para alterações AWS Config de configuração
CIS v1.4.0	4.10 Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de grupo de segurança	[CloudWatch.10] Certifique-se de que exista um filtro métrico de log e um alarme para alterações no grupo de segurança
CIS v1.4.0	4.11 Garanta que um filtro e um alarme de métrica de log existem para alterações em listas de controle de acesso à rede (NACL)	[CloudWatch.11] Certifique-se de que exista um filtro métrico de registro e um alarme para alterações nas listas de controle de acesso à rede (NACL)

Padrão	ID e título do controle padrão	ID e título do controle de segurança
CIS v1.4.0	4.12 Garanta que um filtro e um alarme de métrica de logs existem para alterações em gateways de rede	[CloudWatch.12] Certifique-se de que exista um filtro métrico de log e um alarme para alterações nos gateways de rede
CIS v1.4.0	4.13 Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de tabela de rotas	[CloudWatch.13] Certifique-se de que exista um filtro métrico de log e um alarme para alterações na tabela de rotas
CIS v1.4.0	4.14 Certifique-se de que um filtro e um alarme de métrica de logs existam para alterações de VPC	[CloudWatch.14] Certifique-se de que exista um filtro métrico de log e um alarme para alterações de VPC
CIS v1.4.0	5.1 Garanta que nenhuma ACL de rede permita a entrada de 0.0.0.0/0 para as portas de administração do servidor remoto	As ACLs de rede não devem permitir a entrada de 0.0.0.0/0 para a porta 22 ou porta 3389
CIS v1.4.0	5.3 Verifique se o grupo de segurança padrão de cada VPC restringe todo o tráfego	[EC2.2] O grupo de segurança padrão da VPC não deve permitir o tráfego de entrada e saída
PCI DSS v3.2.1	FOTO. AutoScaling.1 Os grupos de escalonamento automático associados a um balanceador de carga devem usar verificações de integridade do balanceador de carga	[AutoScaling.1] Grupos de Auto Scaling associados a um balanceador de carga devem usar verificações de integridade do ELB
PCI DSS v3.2.1	FOTO. CloudTrail.1 CloudTrail Os registros devem ser criptografados em repouso usando AWS KMS CMKs	[CloudTrail.2] CloudTrail deve ter a criptografia em repouso ativada
PCI DSS v3.2.1	FOTO. CloudTrail.2 CloudTrail deve ser ativado	[CloudTrail.3] Pelo menos uma CloudTrail trilha deve ser ativada

Padrão	ID e título do controle padrão	ID e título do controle de segurança
PCI DSS v3.2.1	FOTO. CloudTrail.3 A validação do arquivo de CloudTrail log deve estar ativada	[CloudTrail.4] a validação do arquivo de CloudTrail log deve estar ativada
PCI DSS v3.2.1	FOTO. CloudTrail.4 CloudTrail trilhas devem ser integradas ao Amazon CloudWatch Logs	[CloudTrail.5] CloudTrail trilhas devem ser integradas com o Amazon CloudWatch Logs
PCI DSS v3.2.1	FOTO. CodeBuild.1 CodeBuild GitHub ou os URLs do repositório de origem do Bitbucket devem usar OAuth	[CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais
PCI DSS v3.2.1	FOTO. CodeBuild.2 As variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado	[CodeBuild.2] as variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado
PCI DSS v3.2.1	O PCI.config.1 deve estar ativado AWS Config	[Config.1] AWS Config deve estar habilitado
PCI DSS v3.2.1	PCI.CW.1 Um filtro de métrica de log e um alarme devem existir para o uso do usuário "raiz"	[CloudWatch.1] Um filtro métrico de log e um alarme devem existir para uso do usuário “root”
PCI DSS v3.2.1	PCI.DMS.1 As instâncias de replicação do Database Migration Service não devem ser públicas	As instâncias de replicação do PCI.DMS.1 Database Migration Service não devem ser públicas
PCI DSS v3.2.1	PCI.EC2.1 Os snapshots do ebs não devem ser restauráveis publicamente	[PCI.EC2.1] Os instantâneos do Amazon EBS não devem ser restauráveis publicamente
PCI DSS v3.2.1	PCI.EC2.2 O grupo de segurança padrão da VPC deve proibir o tráfego de entrada e de saída	[EC2.2] O grupo de segurança padrão da VPC não deve permitir o tráfego de entrada e saída

Padrão	ID e título do controle padrão	ID e título do controle de segurança
PCI DSS v3.2.1	CI.EC2.4 Os EIPs do EC2 não utilizados devem ser removidos	[PCI.EC2.4] Os EIPs do EC2 não utilizados devem ser removidos
PCI DSS v3.2.1	PCI.EC2.5Os grupo de segurança não devem permitir de 0.0.0.0/0 na porta 22	[EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22
PCI DSS v3.2.1	PCI.EC2.6 O registro em log do fluxo de VPC deve ser ativado em todas as VPCs	[EC2.6] O registro de fluxo de VPC deve ser ativado em todas as VPCs
PCI DSS v3.2.1	ELBv2.1 O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS	[ELBv2.1] O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS
PCI DSS v3.2.1	PCI.ES.1 Os domínios do Elasticse arch devem estar em uma VPC	[ES.2] Os domínios do Elasticse arch não devem ser publicamente acessíveis
PCI DSS v3.2.1	PCI.ES.2 Os domínios do Elasticse arch devem ter a criptografia em repouso habilitada	[ES.1] Os domínios do devem ter a criptografia em repouso habilitada.
PCI DSS v3.2.1	FOTO. GuardDuty.1 GuardDuty deve ser ativado	[GuardDuty.1] GuardDuty deve ser ativado
PCI DSS v3.2.1	PCI.IAM.1 A chave de acesso do usuário raiz do IAM não deve existir	[IAM.4] A chave de acesso do usuário raiz do não deve existir
PCI DSS v3.2.1	PCI.IAM.2 Os usuários do IAM não devem ter políticas do IAM anexadas	[IAM.2] Os usuários do não devem ter políticas do IAM anexadas
PCI DSS v3.2.1	PCI.IAM.3 As políticas do IAM não devem permitir privilégios administr ativos completos "*"	[IAM.1] As políticas do não devem permitir privilégios administrativos completos "*"

Padrão	ID e título do controle padrão	ID e título do controle de segurança
PCI DSS v3.2.1	PCI.IAM.4 A MFA de hardware deve estar habilitada para o usuário raiz	[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
PCI DSS v3.2.1	PCI.IAM.5 A MFA virtual deve estar habilitada para o usuário raiz	[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
PCI DSS v3.2.1	PCI.IAM.6 A MFA deve estar habilitada para todos os usuários do IAM	[PCI.IAM.6] A MFA deve estar habilitada para todos os usuários do
PCI DSS v3.2.1	PCI.IAM.7 As credenciais de usuário do IAM devem ser desativadas se não forem usadas dentro de um número predefinido de dias	As credenciais de usuário do IAM não utilizadas devem ser removidas
PCI DSS v3.2.1	PCI.IAM.8 Políticas de senha para usuários do IAM que devem ter configurações fortes	[IAM.10] As políticas de senha para usuários do IAM devem ter durações fortes AWS Config
PCI DSS v3.2.1	PCI.KMS.1 A alternância da chave mestra do cliente (CMK) deve estar habilitada	A rotação de AWS KMS teclas [KMS.4] deve estar ativada
PCI DSS v3.2.1	PCI.lambda.1 As funções do Lambda devem proibir o acesso público	[PCI.lambda.1] As funções do devem proibir o acesso público
PCI DSS v3.2.1	PCI.Lambda.2 As funções do Lambda devem estar em uma VPC	[PCI.Lambda.2] As funções do Lambda devem estar em uma VPC
PCI DSS v3.2.1	Os domínios PCI.OpenSearch.1 OpenSearch devem estar em uma VPC	Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público
PCI DSS v3.2.1	PCI.Opensearch.2 Os instantâneos do EBS não devem ser restauráveis publicamente	Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada

Padrão	ID e título do controle padrão	ID e título do controle de segurança
PCI DSS v3.2.1	PCI.RDS.1 Os instantâneos do RDS devem ser privados	[RDS.1] Os instantâneos do RDS devem ser privados
PCI DSS v3.2.1	PCI.RDS.2 As instâncias de banco de dados do RDS devem proibir o acesso público	[RDS.2] As instâncias de banco de dados do RDS devem proibir o acesso público, conforme determina do pela duração PubliclyAccessible AWS Config
PCI DSS v3.2.1	PCI.Redshift.1 Os clusters do Amazon Redshift devem proibir o acesso público	[PCI.Redshift.1] Os clusters do devem proibir o acesso público
PCI DSS v3.2.1	PCI.S3.1 Os buckets do S3 devem proibir o acesso público à gravação	[S3.3] Os buckets de uso geral do S3 devem bloquear o acesso público de gravação
PCI DSS v3.2.1	PCI.S3.2 Os buckets do S3 devem proibir o acesso público à leitura	[S3.2] Os buckets de uso geral do S3 devem bloquear o acesso público de leitura
PCI DSS v3.2.1	PCI.S3.3 Os buckets do S3 devem ter a replicação entre regiões ativada	[S3.7] Os buckets de uso geral do S3 devem usar a replicação entre regiões
PCI DSS v3.2.1	PCI.S3.5 Os buckets do S3 devem exigir solicitações para usar o Secure Socket Layer	[S3.5] Os buckets de uso geral do S3 devem exigir solicitações de uso de SSL
PCI DSS v3.2.1	PCI.S3.6 A configuração do S3 Block Public Access deve estar habilitada	[S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas
PCI DSS v3.2.1	FOTO. SageMaker.1 As instância s de SageMaker notebooks da Amazon não devem ter acesso direto à Internet	[SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet

Padrão	ID e título do controle padrão	ID e título do controle de segurança
PCI DSS v3.2.1	PCI.SSM.1 As instâncias do gerenciadas pelo devem ter um status de conformidade de patch de COMPLIANT após a instalação do patch	[PCI.SSM.1] As instâncias do Amazon EC2 gerenciadas pelo devem ter um status de conformidade de patch de COMPLIANT (Em conformidade) após a instalação do patch
PCI DSS v3.2.1	PCI.SSM.2 As instâncias de EC2 gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL	PCI.SSM.2 As instâncias de Amazon EC2 gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
PCI DSS v3.2.1	As instâncias PCI.SSM.3 EC2 devem ser gerenciadas por AWS Systems Manager	[SSM.1] As instâncias do Amazon EC2 devem ser gerenciadas por AWS Systems Manager

Atualização de fluxos de trabalho para consolidação

Se os seus fluxos de trabalho não dependem do formato específico de nenhum campo de descoberta de controle, nenhuma ação é necessária.

Se seus fluxos de trabalho dependerem do formato específico de qualquer campo de localização de controle anotado nas tabelas, você deverá atualizar seus fluxos de trabalho. Por exemplo, se você criou uma regra do Amazon CloudWatch Events que acionou uma ação para um ID de controle específico (como invocar uma AWS Lambda função se o ID de controle for igual ao CIS 2.7), atualize a regra para usar CloudTrail .2, o `Compliance.SecurityControlId` campo desse controle.

Se você criou insights personalizados usando qualquer um dos campos de busca de controle ou valores que foram alterados, atualize esses insights para usar os campos ou valores atuais.

Exemplos de ASFF

As seções a seguir contêm exemplos de atributos obrigatórios e opcionais no AWS Security Finding Format (ASFF), bem como exemplos de cada recurso suportado pelo ASFF.

Tópicos

Atributos de nível superior necessários

Os seguintes atributos de nível superior no AWS Security Finding Format (ASFF) são necessários para todas as descobertas no Security Hub. Para obter mais informações sobre esses atributos obrigatórios, consulte AwsSecurityFinding na Referência da API do AWS Security Hub .

AwsAccountId

O Conta da AWS ID ao qual a descoberta se aplica.

Exemplo

```
"AwsAccountId": "111111111111"
```

CreatedAt

Indica quando o possível problema de segurança detectado por uma descoberta foi criado.

Exemplo

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

> **Note**
>
> O Security Hub exclui descobertas 90 dias após a atualização mais recente ou 90 dias após a data de criação, se não houver atualização. Para armazenar descobertas por mais de 90 dias, você pode configurar uma regra na Amazon EventBridge que encaminha as descobertas para o seu bucket do S3.

Descrição

A descrição de uma descoberta. Esse campo pode ser um texto padronizado não específico ou detalhes específicos da instância da descoberta.

Para as descobertas de controle geradas pelo Security Hub, esse campo fornece uma descrição do controle.

Esse campo não faz referência a um padrão se você ativar as descobertas de controle consolidadas.

Exemplo

```
"Description": "This AWS control checks whether AWS Config is enabled in the current
 account and Region."
```

GeneratorId

O identificador do componente específico da solução (uma unidade discreta de lógica) que gerou uma descoberta.

Para as descobertas de controle que o Security Hub gera, esse campo não faz referência a um padrão se você ativar as constatações de controle consolidadas.

Exemplo

```
"GeneratorId": "security-control/Config.1"
```

Id

O identificador específico do produto para uma descoberta. Para descobertas de controle geradas pelo Security Hub, esse campo fornece o nome do recurso da Amazon (ARN) da descoberta.

Esse campo não faz referência a um padrão se você ativar as descobertas de controle consolidadas.

Exemplo

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/
ab6d6a26-a156-48f0-9403-115983e5a956

"
```

ProductArn

O nome do recurso da Amazon (ARN) gerado pelo Security Hub que identifica exclusivamente um produto de descobertas de terceiros depois que o produto é registrado com o Security Hub.

O formato desse campo é `arn:`*`partition`*`:securityhub:`*`region`*`:`*`account-id`*`:product/`*`company-id`*`/`*`product-id`*.

- Para AWS serviços integrados ao Security Hub, o `company-id` deve ser "`aws`“e o `product-id` deve ser o nome do serviço AWS público. Como AWS os produtos e serviços não estão associados a uma conta, a `account-id` seção do ARN está vazia. AWS serviços que ainda não estão integrados ao Security Hub são considerados produtos de terceiros.
- Para produtos públicos, o `company-id` e o `product-id` devem ser os valores de ID especificados no momento do registro.
- Para os produtos privados, o `company-id` deve ser o ID da conta. O `product-id` deve ser a palavra reservada "default" ou o ID que foi especificado no momento do registro.

Exemplo

```
// Private ARN
    "ProductArn": "arn:aws:securityhub:us-east-1:111111111111:product/111111111111/
default"

// Public ARN

    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty"
    "ProductArn": "arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-
pro"
```

Recursos

O `Resources`objeto fornece um conjunto de tipos de dados de recursos que descrevem os AWS recursos aos quais a descoberta se refere.

Exemplo

```
"Resources": [
  {
    "ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0",
    "ApplicationName": "SampleApp",
    "DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
```

```
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
                        }
                    },
                    {
                        "Count": 59,
                        "Type": "EMAIL_ADDRESS",
                        "Occurrences": {
                            "Pages": [
                                {
                                    "PageNumber": 1,
                                    "OffsetRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                     },
                                    "LineRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                    }
                                }
                            ]
                        }
                    },
```

```
                    {
                        "Count": 2229,
                        "Type": "URL",
                        "Occurrences": {
                           "LineRanges": [
                               {
                                   "Start": 1,
                                   "End": 13
                               }
                           ]
                        }
                    },
                    {
                        "Count": 13826,
                        "Type": "NameDetection",
                        "Occurrences": {
                            "Records": [
                                {
                                    "RecordIndex": 1,
                                    "JsonPath": "$.ssn.value"
                                }
                            ]
                        }
                    },
                    {
                        "Count": 32,
                        "Type": "AddressDetection"
                    }
                ],
                "TotalCount": 32
            }
        ],
        "CustomDataIdentifiers": {
            "Detections": [
                {
                    "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                    "Name": "1712be25e7c7f53c731fe464f1c869b8",
                    "Count": 2,
                }
            ],
            "TotalCount": 2
        }
    }
},
```

```
 "Type": "AwsEc2Instance",
 "Id": "arn:aws:ec2:us-west-2:123456789012:instance/i-abcdef01234567890",
 "Partition": "aws",
 "Region": "us-west-2",
 "ResourceRole": "Target",
 "Tags": {
  "billingCode": "Lotus-1-2-3",
  "needsPatching": true
 },
 "Details": {
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
  "ImageId": "ami-79fd7eee",
  "IpV4Addresses": ["1.1.1.1"],
  "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
  "KeyName": "testkey",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "MetadataOptions": {
   "HttpEndpoint": "enabled",
   "HttpProtocolIpv6": "enabled",
   "HttpPutResponseHopLimit": 1,
   "HttpTokens": "optional",
   "InstanceMetadataTags": "disabled"
  }
 },
  "NetworkInterfaces": [
  {
   "NetworkInterfaceId": "eni-e5aa89a3"
  }
  ],
  "SubnetId": "PublicSubnet",
  "Type": "i3.xlarge",
  "VirtualizationType": "hvm",
  "VpcId": "TestVPCIpv6"
 }

]
```

SchemaVersion

A versão do esquema para a qual uma descoberta está formatada. O valor desse campo deve ser uma das versões publicadas oficialmente identificadas pela AWS. Na versão atual, a versão do esquema AWS Security Finding Format é`2018-10-08`.

Exemplo

```
"SchemaVersion": "2018-10-08"
```

Gravidade

Define a importância de uma descoberta. Para obter detalhes sobre esse objeto, consulte `Severity` na Referência da API AWS Security Hub .

`Severity` é ao mesmo tempo um objeto de nível superior em uma descoberta e está aninhado sob o objeto `FindingProviderFields`.

O valor do objeto `Severity` de nível superior para uma descoberta só deve ser atualizado pela API `BatchUpdateFindings`.

Para fornecer informações de gravidade, os provedores de descobertas devem atualizar o objeto `Severity` em `FindingProviderFields` quando fizerem uma solicitação de API `BatchImportFindings`.
Se uma solicitação `BatchImportFindings` para uma nova descoberta fornecer apenas `Label` ou fornecer apenas `Normalized`, o Security Hub preencherá automaticamente o valor do outro campo. O campo `Product` sob `FindingProviderFields` foi descontinuado e não é preenchido nas descobertas atuais. No lugar dela, use o campo `Original`.

A gravidade da descoberta não considera a criticidade dos ativos envolvidos ou do recurso subjacente. A criticidade é definida como o nível de importância dos recursos associados à descoberta. Por exemplo, um recurso associado a um aplicativo de missão crítica tem maior criticidade do que um recurso associado a testes de não produção. Para capturar informações sobre criticidade do recurso, use o campo `Criticality`.

Recomendamos usar a seguinte orientação ao traduzir os escores de gravidade nativos dos resultados para o valor de `Severity.Label` na ASFF.

- `INFORMATIONAL` — Essa categoria pode incluir uma descoberta para uma verificação `PASSED`, `WARNING` ou `NOT AVAILABLE` ou uma identificação de dados confidenciais.
- `LOW` — Descobertas que podem resultar em compromissos futuros. Por exemplo, essa categoria pode incluir vulnerabilidades, pontos fracos da configuração e senhas expostas.
- `MEDIUM`: as descobertas que indicam um comprometimento ativo, mas nenhuma indicação de que um adversário tenha concluído seus objetivos. Por exemplo, essa categoria pode incluir atividade de malware, atividade de hacking e detecção de comportamento incomum.

- `HIGH` ou `CRITICAL`: descobertas que indicam que um adversário concluiu seus objetivos, como perda ou comprometimento ativo de dados ou uma negação de serviço.

Exemplo

```
"Severity": {
    "Label": "CRITICAL",
    "Normalized": 90,
    "Original": "CRITICAL"
}
```

Cargo

O título de uma descoberta. Esse campo pode conter texto padronizado não específico ou detalhes específicos dessa instância da descoberta.

Para descobertas de controle, esse campo fornece o título do controle.

Esse campo não faz referência a um padrão se você ativar as descobertas de controle consolidadas.

Exemplo

```
"Title": "AWS Config should be enabled"
```

Tipos

Um ou mais tipos de descobertas no formato de *namespace*/*category*/*classifier* que classificam uma descoberta. Esse campo não faz referência a um padrão se você ativar as descobertas de controle consolidadas.

`Types` só deve ser atualizado usando `BatchUpdateFindings`.

Os provedores de descobertas que desejam fornecer um valor para `Types` devem usar o atributo `Types` sob `FindingProviderFields`.

Na lista a seguir, os marcadores de nível superior são namespaces, os marcadores de segundo nível são categorias e os marcadores de terceiro nível são classificadores. Recomendamos que os provedores de descobertas usem namespaces definidos para ajudar a classificar e agrupar as descobertas. As categorias e os classificadores definidos também podem ser usados, mas não são

obrigatórios. Somente o namespace Verificações de software e configuração tem classificadores definidos.

É possível definir um caminho parcial para namespace/category/classifier. Por exemplo, todos os tipos de descoberta a seguir são válidos:

- TTPs
- TTPs/Evasão de defesa
- TTPS/Evasão de defesa/ CloudTrailStopped

As categorias de táticas, técnicas e procedimentos (TTPs) na lista a seguir se alinham com a MITRE ATT&CK MatrixTM. O spacename de Comportamentos incomuns reflete o comportamento incomum geral, como anomalias estatísticas gerais, e não está alinhado a um TTP específico. Entretanto, é possível classificar uma descoberta com os tipos de descoberta Comportamentos incomuns e TTPs.

Lista de namespaces, categorias e classificadores:

- Verificações de software e configuração
  - Vulnerabilidades
    - CVE
  - AWS Melhores práticas de segurança
    - Acessibilidade de rede
    - Análise de comportamento do tempo de execução
  - Padrões regulatórios e do setor
    - AWS Melhores práticas básicas de segurança
    - Referências do CIS Host Hardening
    - Referência do CIS AWS Foundations
    - PCI-DSS
    - Controles da Cloud Security Alliance
    - Controles ISO 90001
    - Controles ISO 27001
    - Controles ISO 27017
    - Controles ISO 27018
    - SOC 1

    - SOC 2
    - Controles HIPAA (EUA)
    - Controles NIST 800-53 (EUA)
    - Controles da CSF do NIST (EUA)
    - Controles IRAP (Austrália)
    - Controles K-ISMS (Coreia)
    - Controles MTCS (Singapura)
    - Controles FISC (Japão)
    - Controles da Lei Meu Número (Japão)
    - Controles ENS (Espanha)
    - Controles Cyber Essentials Plus (Reino Unido)
    - Controles G-Cloud (Reino Unido)
    - Controles C5 (Alemanha)
    - Controles IT-Grundschutz (Alemanha)
    - Controles GDPR (Europa)
    - Controles TISAX (Europa)
  - Gerenciamento de patches
- TTPs
  - Acesso inicial
  - Execução
  - Persistência
  - Escalonamento de privilégios
  - Evasão de defesa
  - Acesso credencial
  - Descoberta
  - Movimento lateral
  - Coleta
  - Comando e controle
- Efeitos
  - Exposição de dados

  - Exfiltração de dados
  - Destruição de dados
  - Negação de serviço
  - Consumo de recursos
- Comportamentos incomuns
  - Aplicativo
  - Fluxo de rede
  - Endereço IP
  - Usuário
  - VM
  - Contêiner
  - Sem servidor
  - Processar
  - Banco de dados
  - Dados
- Identificação de dados confidenciais
  - PII
  - Senhas
  - Legal
  - Financeiro
  - Segurança
  - Business

Exemplo

```
"Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
    ]
```

UpdatedAt

Indica quando o provedor de descoberta atualizou o registro de descoberta pela última vez.

Esse timestamp reflete a hora em que o registro de descoberta foi atualizado pela última vez ou a mais recente. Consequentemente, ele pode ser diferente do timestamp `LastObservedAt`, que reflete quando o evento ou vulnerabilidade foi observado pela última vez ou foi observado mais recentemente.

Ao atualizar o registro de descoberta, é necessário atualizar esse timestamp para o timestamp atual. Após a criação de um registro de descoberta, os timestamps `CreatedAt` e `UpdatedAt` devem ser o mesmo. Após uma atualização do registro de localização, o valor desse campo deve ser mais recente do que todos os valores anteriores que ele continha.

Observe que `UpdatedAt` não pode ser atualizado usando a operação da API `BatchUpdateFindings`. Você só pode atualizá-lo usando `BatchImportFindings`.

Exemplo

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

> **Note**
>
> O Security Hub exclui descobertas 90 dias após a atualização mais recente ou 90 dias após a data de criação, se não houver atualização. Para armazenar descobertas por mais de 90 dias, você pode configurar uma regra na Amazon EventBridge que encaminha as descobertas para o seu bucket do S3.

Atributos opcionais de nível superior

Esses atributos de nível superior são opcionais no AWS Security Finding Format (ASFF). Para obter mais informações sobre esses atributos, consulte AwsSecurityFindinga Referência AWS Security Hub da API.

Ação

O objeto `Action` fornece detalhes sobre uma ação que afeta ou que foi executada em um recurso.

Exemplo

```
"Action": {
```

```
    "ActionType": "PORT_PROBE",
    "PortProbeAction": {
        "PortProbeDetails": [
            {
                "LocalPortDetails": {
                    "Port": 80,
                    "PortName": "HTTP"
                  },
                "LocalIpDetails": {
                     "IpAddressV4": "192.0.2.0"
                 },
                "RemoteIpDetails": {
                    "Country": {
                        "CountryName": "Example Country"
                    },
                    "City": {
                        "CityName": "Example City"
                    },
                   "GeoLocation": {
                       "Lon": 0,
                       "Lat": 0
                   },
                   "Organization": {
                       "AsnOrg": "ExampleASO",
                       "Org": "ExampleOrg",
                       "Isp": "ExampleISP",
                       "Asn": 64496
                   }
                }
            }
        ],
        "Blocked": false
    }
}
```

AwsAccountName

O Conta da AWS nome ao qual a descoberta se aplica.

Exemplo

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

O nome da empresa do produto que gerou a descoberta. Para descobertas baseadas em controle, a empresa é AWS.

O Security Hub preenche esse atributo automaticamente para cada descoberta. Você não pode atualizá-lo usando `BatchImportFindings` ou `BatchUpdateFindings`. A exceção a isso é quando você utiliza uma integração personalizada. Consulte the section called “Usar integrações de produtos personalizados”.

Ao usar o console do Security Hub para filtrar as descobertas pelo nome da empresa, você usa esse atributo. Ao usar o console do Security Hub para filtrar as descobertas pelo nome da empresa, você usa o atributo `aws/securityhub/CompanyName` em `ProductFields`. O Security Hub não sincroniza esses dois atributos.

Exemplo

```
"CompanyName": "AWS"
```

Conformidade

O objeto `Compliance` fornece detalhes da descoberta relacionada a um controle. Esse atributo é retornado para descobertas geradas a partir de um controle do Security Hub e para descobertas AWS Config enviadas ao Security Hub.

Exemplo

```
"Compliance": {
    "AssociatedStandards": [
        {"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
        {"StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
        {"StandardsId": "standards/nist-800-53/v/5.0.0"}
    ],
    "RelatedRequirements": [
        "NIST.800-53.r5 AC-4",
        "NIST.800-53.r5 AC-4(21)",
        "NIST.800-53.r5 SC-7",
        "NIST.800-53.r5 SC-7(11)",
        "NIST.800-53.r5 SC-7(16)",
        "NIST.800-53.r5 SC-7(21)",
        "NIST.800-53.r5 SC-7(4)",
```

```
        "NIST.800-53.r5 SC-7(5)"
    ],
    "SecurityControlId": "EC2.18",
    "SecurityControlParameters":[
        {
            "Name": "authorizedTcpPorts",
            "Value": ["80", "443"]
        },
        {
            "Name": "authorizedUdpPorts",
            "Value": ["427"]
        }
    ],
    "Status": "NOT_AVAILABLE",
    "StatusReasons": [
        {
            "ReasonCode": "CONFIG_RETURNS_NOT_APPLICABLE",
            "Description": "This finding has a compliance status of NOT AVAILABLE
 because AWS Config sent Security Hub a finding with a compliance state of Not
 Applicable. The potential reasons for a Not Applicable finding from Config are that
 (1) a resource has been moved out of scope of the Config rule; (2) the Config rule has
 been deleted; (3) the resource has been deleted; or (4) the logic of the Config rule
 itself includes scenarios where Not Applicable is returned. The specific reason why
 Not Applicable is returned is not available in the Config rule evaluation."
        }
    ]
}
```

Confiança

A probabilidade de que uma descoberta identifique com precisão o comportamento ou o problema que se pretendia identificar.

`Confidence` só deve ser atualizado usando `BatchUpdateFindings`.

Os provedores de descobertas que desejam fornecer um valor para `Confidence` devem usar o atributo `Confidence` sob `FindingProviderFields`. Consulte the section called “Usar o FindingProviderFields”.

`Confidence` é pontuado em uma base de 0 a 100 usando uma escala de proporção. 0 significa 0% de confiança e 100 significa 100% de confiança. Por exemplo, uma detecção de exfiltração de dados baseada em um desvio estatístico do tráfego de rede tem baixa confiança porque uma exfiltração real não foi verificada.

Exemplo

```
"Confidence": 42
```

Criticidade

O nível de importância atribuído aos recursos associados a uma descoberta.

`Criticality` só deve ser atualizado chamando a operação da API `BatchUpdateFindings`. Não atualize este objeto com `BatchImportFindings`.

Os provedores de descobertas que desejam fornecer um valor para `Criticality` devem usar o atributo `Criticality` sob `FindingProviderFields`. Consulte the section called “Usar o FindingProviderFields”.

`Criticality` é pontuado em uma base de 0 a 100, usando uma escala de proporção que suporta somente números inteiros completos. Uma pontuação de 0 significa que os recursos subjacentes não têm criticidade e uma pontuação de 100 é reservada para os recursos mais críticos.

Para cada recurso, considere o seguinte ao atribuir `Criticality`:

- O recurso afetado contém dados confidenciais (por exemplo, um bucket do S3 com PII)?
- O recurso afetado permite que um adversário aprofunde o acesso ou estenda os recursos dele para realizar outras atividades maliciosas (por exemplo, uma conta sysadmin comprometida)?
- O recurso é um ativo crítico para os negócios (por exemplo, um sistema comercial importante que, se comprometido, poderia ter um impacto significativo na receita)?

É possível usar as seguintes diretrizes:

- Um recurso que alimenta sistemas de missão crítica ou contém dados altamente confidenciais pode ser classificado na faixa de 75 a 100.
- Um recurso que alimenta sistemas importantes (mas não críticos) ou que contém dados moderadamente importantes pode ser pontuado na faixa de 25 a 74.
- Um recurso que alimenta sistemas sem importância ou contém dados não confidenciais deve ser pontuado na faixa de 0 a 24.

Exemplo

```
"Criticality": 99
```

FindingProviderFields

`FindingProviderFields` inclui os seguintes atributos:

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

É possível atualizar `FindingProviderFields` usando a operação da API `BatchImportFindings`. Você não pode atualizá-lo com `BatchUpdateFindings`.

Para obter detalhes sobre como o Security Hub lida com atualizações de `BatchImportFindings` a `FindingProviderFields` para os atributos de nível superior correspondentes, consulte the section called “Usar o FindingProviderFields”.

Exemplo

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

FirstObservedAt

Indica quando o possível problema de segurança detectado por uma descoberta foi observado pela primeira vez.

Esse timestamp reflete a hora em que o evento ou a vulnerabilidade foi observado pela primeira vez. Consequentemente, ele pode ser diferente do timestamp `CreatedAt`, que reflete a hora em que esse registro de descoberta foi criado.

Este timestamp deve ser imutável entre as atualizações do registro de descoberta, mas pode ser atualizado se um timestamp mais preciso tiver sido determinado.

Exemplo

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

Indica quando o possível problema de segurança detectado por uma descoberta foi observado mais recentemente pelo produto de descobertas de segurança.

Esse timestamp reflete a hora em que o evento ou a vulnerabilidade foi observado pela última vez ou mais recentemente. Consequentemente, ele pode ser diferente do timestamp `UpdatedAt`, que reflete quando esse registro de descoberta foi atualizado pela última vez ou mais recentemente.

É possível fornecer esse timestamp, mas isso não é obrigatório na primeira observação. Se você fornecer este campo na primeira observação, o timestamp deverá ser igual ao `FirstObservedAt`. Você deve atualizar esse campo para refletir o último ou o mais recente timestamp observado sempre que uma descoberta for observada.

Exemplo

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

Malware

O objeto `Malware` fornece uma lista de malware relacionado a uma descoberta.

Exemplo

```
"Malware": [
```

```
    {
        "Name": "Stringler",
        "Type": "COIN_MINER",
        "Path": "/usr/sbin/stringler",
        "State": "OBSERVED"
    }
]
```

Network (retirado)

O objeto `Network` oferece informações relacionadas à rede sobre uma descoberta.

Esse objeto é retirado. Para fornecer esses dados, é possível mapear os dados para um recurso em `Action` ou usar o objeto `Resources`.

Exemplo

```
"Network": {
    "Direction": "IN",
    "OpenPortRange": {
        "Begin": 443,
        "End": 443
    },
    "Protocol": "TCP",
    "SourceIpV4": "1.2.3.4",
    "SourceIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "SourcePort": "42",
    "SourceDomain": "example1.com",
    "SourceMac": "00:0d:83:b1:c0:8e",
    "DestinationIpV4": "2.3.4.5",
    "DestinationIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "DestinationPort": "80",
    "DestinationDomain": "example2.com"
}
```

NetworkPath

O objeto `NetworkPath` fornece informações sobre um caminho de rede relacionado a uma descoberta. Cada entrada em `NetworkPath` representa um componente do caminho.

Exemplo

```
"NetworkPath" : [
```

```
    {
        "ComponentId": "abc-01a234bc56d8901ee",
        "ComponentType": "AWS::EC2::InternetGateway",
        "Egress": {
            "Destination": {
                "Address": [ "192.0.2.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": ["203.0.113.0/24"]
            }
        },
        "Ingress": {
            "Destination": {
                "Address": [ "198.51.100.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                 ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": [ "203.0.113.0/24" ]
            }
        }
     }
]
```

Observação

O objeto `Note` especifica uma nota definida pelo usuário que pode ser adicionado a uma descoberta.

Um provedor de descoberta pode fornecer uma nota inicial para uma descoberta, mas não pode adicionar notas depois disso. Uma nota só pode ser atualizada usando `BatchUpdateFindings`.

Exemplo

```
"Note": {
    "Text": "Don't forget to check under the mat.",
    "UpdatedBy": "jsmith",
    "UpdatedAt": "2018-08-31T00:15:09Z"
}
```

PatchSummary

O objeto `PatchSummary` fornece um resumo do status de conformidade do patch de uma instância em relação a um padrão de conformidade selecionado.

Exemplo

```
"PatchSummary" : {
    "FailedCount" : 0,
    "Id" : "pb-123456789098",
    "InstalledCount" : 100,
    "InstalledOtherCount" : 1023,
    "InstalledPendingReboot" : 0,
    "InstalledRejectedCount" : 0,
    "MissingCount" : 100,
    "Operation" : "Install",
    "OperationEndTime" : "2018-09-27T23:39:31Z",
    "OperationStartTime" : "2018-09-27T23:37:31Z",
    "RebootOption" : "RebootIfNeeded"
}
```

Processar

O objeto `Process` fornece detalhes relacionados ao processo sobre a descoberta.

Exemplo:

```
"Process": {
    "LaunchedAt": "2018-09-27T22:37:31Z",
    "Name": "syslogd",
    "ParentPid": 56789,
    "Path": "/usr/sbin/syslogd",
    "Pid": 12345,
    "TerminatedAt": "2018-09-27T23:37:31Z"
}
```

ProcessedAt

Indica quando o Security Hub recebeu uma descoberta e começa a processá-la.

Isso difere de `CreatedAt` e `UpdatedAt`, que são timestamps obrigatórios relacionados à interação do provedor de busca com o problema de segurança e a descoberta. O timestamp `ProcessedAt` indica quando o Security Hub começa a processar uma descoberta. Uma descoberta aparece na conta do usuário após a conclusão do processamento.

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

Um tipo de dados em que os produtos de descobertas de segurança podem incluir detalhes adicionais específicos da solução que não fazem parte do Formato de descoberta de AWS segurança definido.

Para descobertas geradas pelos controles do Security Hub, `ProductFields` inclui informações sobre o controle. Consulte the section called “Gerando e atualizando descobertas de controle”.

Esse campo não deve conter dados redundantes e não deve conter dados que entrem em conflito com os campos do Formato AWS de descoberta de segurança.

O prefixo `aws/` "" representa um namespace reservado somente para AWS produtos e serviços e não deve ser enviado com descobertas de integrações de terceiros.

Embora não seja obrigatório, os produtos devem formatar nomes de campos como `company-id/product-id/field-name`, em que o `company-id` e o `product-id` correspondem aos produtos fornecidos no `ProductArn` da descoberta.

Os campos de referência a `Archival` são usados quando o Security Hub arquiva uma descoberta existente. Por exemplo, o Security Hub arquiva descobertas existentes quando você desabilita um controle ou padrão e quando você ativa ou desativa descobertas de controle consolidadas.

Esse campo também pode incluir informações sobre o padrão que inclui o controle que produziu a descoberta.

Exemplo

```
"ProductFields": {
```

```
    "API", "DeleteTrail",
    "ArchivalReasons:0/Description": "The finding is in an ARCHIVED state because
 consolidated control findings has been turned on or off. This causes findings in the
 previous state to be archived when new findings are being generated.",
    "ArchivalReasons:0/ReasonCode": "CONSOLIDATED_CONTROL_FINDINGS_UPDATE",
    "aws/inspector/AssessmentTargetName": "My prod env",
    "aws/inspector/AssessmentTemplateName": "My daily CVE assessment",
    "aws/inspector/RulesPackageName": "Common Vulnerabilities and Exposures",
    "generico/secure-pro/Action.Type", "AWS_API_CALL",
    "generico/secure-pro/Count": "6",
    "Service_Name": "cloudtrail.amazonaws.com"
}
```

ProductName

Oferece o nome do produto que gerou a descoberta. Para descobertas baseadas em controle, o nome do produto é Security Hub.

O Security Hub preenche esse atributo automaticamente para cada descoberta. Você não pode atualizá-lo usando `BatchImportFindings` ou `BatchUpdateFindings`. A exceção a isso é quando você utiliza uma integração personalizada. Consulte the section called “Usar integrações de produtos personalizados”.

Ao usar o console do Security Hub para filtrar as descobertas pelo nome do produto, você usa esse atributo.

Ao usar o console do Security Hub para filtrar as descobertas pelo nome do produto, você usa o atributo `aws/securityhub/ProductName` em `ProductFields`.

O Security Hub não sincroniza esses dois atributos.

RecordState

Fornece o registro de uma descoberta.

Por padrão, quando inicialmente geradas por um serviço, as descobertas são consideradas como `ACTIVE`.

O estado `ARCHIVED` indica que uma descoberta deve ser ocultada da exibição. As descobertas arquivadas não são excluídas imediatamente. É possível pesquisar, revisar e gerar relatórios sobre elas. O Security Hub arquiva automaticamente as constatações baseadas em controle se o recurso associado for excluído, se o recurso não existir ou se o controle for desativado.

`RecordState` é destinado a provedores de descobertas e só pode ser atualizado por `BatchImportFindings`. Você não pode atualizá-lo usando `BatchUpdateFindings`.

Para rastrear o status de sua investigação sobre uma descoberta, use `Workflow` em vez de `RecordState`.

Se o estado do registro mudar de `ARCHIVED` para `ACTIVE` e o status do fluxo de trabalho da descoberta for `NOTIFIED` ou `RESOLVED`, o Security Hub definirá automaticamente o status do fluxo de trabalho como `NEW`.

Exemplo

```
"RecordState": "ACTIVE"
```

Região

Especifica a Região da AWS partir da qual a descoberta foi gerada.

O Security Hub preenche esse atributo automaticamente para cada descoberta. Você não pode atualizá-lo usando `BatchImportFindings` ou `BatchUpdateFindings`.

Exemplo

```
"Region": "us-west-2"
```

RelatedFindings

Fornece uma lista de descobertas relacionadas à descoberta atual.

`RelatedFindings` só deve ser atualizado com a operação da API `BatchUpdateFindings`. Você não deve atualizar esse objeto com `BatchImportFindings`.

Para solicitações `BatchImportFindings`, os provedores de descobertas devem usar o objeto `RelatedFindings` sob `FindingProviderFields`.

Para ver as descrições dos atributos `RelatedFindings`, consulte `RelatedFinding`na Referência da API AWS Security Hub .

Exemplo

```
"RelatedFindings": [
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000" },
```

```
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "AcmeNerfHerder-111111111111-x189dx7824" }
]
```

Correção

O objeto `Remediation` fornece informações sobre etapas de correção recomendadas para resolver a descoberta.

Exemplo

```
"Remediation": {
    "Recommendation": {
        "Text": "For instructions on how to fix this issue, see the AWS Security Hub
 documentation for EC2.2.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation"
    }
}
```

Amostra

Especifica se a descoberta é uma descoberta de amostra.

```
"Sample": true
```

SourceUrl

O objeto `SourceUrl` fornece um URL que encaminha para uma página sobre a descoberta atual no produto de descoberta.

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

O objeto `ThreatIntelIndicator` fornece detalhes sobre inteligência de ameaças relacionados a uma descoberta.

Exemplo

```
"ThreatIntelIndicators": [
  {
    "Category": "BACKDOOR",
```

```
    "LastObservedAt": "2018-09-27T23:37:31Z",
    "Source": "Threat Intel Weekly",
    "SourceUrl": "http://threatintelweekly.org/backdoors/8888",
    "Type": "IPV4_ADDRESS",
    "Value": "8.8.8.8",
  }
]
```

Ameaças

O objeto `Threats` fornece detalhes sobre a ameaça detectada por uma descoberta.

Exemplo

```
"Threats": [{
    "FilePaths": [{
        "FileName": "b.txt",
        "FilePath": "/tmp/b.txt",
        "Hash": "sha256",
        "ResourceId": "arn:aws:ec2:us-west-2:123456789012:volume/vol-032f3bdd89aee112f"
    }],
    "ItemCount": 3,
    "Name": "Iot.linux.mirai.vwisi",
    "Severity": "HIGH"
}]
```

UserDefinedFields

Fornece uma lista de pares de string de nome e valor associados à descoberta. Esses são campos personalizados, definidos pelo usuário, que são adicionados a uma descoberta. Esses campos podem ser gerados automaticamente por meio de sua configuração específica.

Os provedores de localização não devem usar esse campo para dados gerados pelo produto. Em vez disso, os provedores de localização podem usar o `ProductFields` campo para dados que não são mapeados para nenhum campo padrão do Formato AWS de Busca de Segurança.

Esses campos só podem ser atualizados usando `BatchUpdateFindings`.

Exemplo

```
"UserDefinedFields": {
    "reviewedByCio": "true",
    "comeBackToLater": "Check this again on Monday"
```

```
}
```

VerificationState

Fornece a veracidade de uma descoberta. Os produtos de descobertas podem fornecer um valor de `UNKNOWN` para esse campo. Um produto de descobertas deve fornecer um valor para esse campo se houver um analógico significativo no sistema do produto de descobertas. Normalmente, esse campo é preenchido por uma determinação ou ação do usuário depois de investigar uma descoberta.

Um provedor de descoberta pode fornecer um valor inicial para esse atributo, mas não pode atualizá-lo depois disso. Esse atributo só pode ser atualizado usando `BatchUpdateFindings`.

```
"VerificationState": "Confirmed"
```

Vulnerabilidades

O objeto `Vulnerabilities` fornece uma lista de vulnerabilidades associadas a uma descoberta.

Exemplo

```
"Vulnerabilities" : [
    {
        "CodeVulnerabilities": [{
            "Cwes": [
                "CWE-798",
                "CWE-799"
            ],
            "FilePath": {
                "EndLine": 421,
                "FileName": "package-lock.json",
                "FilePath": "package-lock.json",
                "StartLine": 420
            },
                "SourceArn":"arn:aws:lambda:us-east-1:123456789012:layer:AWS-AppConfig-
Extension:114"
        }],
        "Cvss": [
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N",
                "Version": "V3"
            },
            {
```

```
                "BaseScore": 4.7,
                "BaseVector": "AV:L/AC:M/Au:N/C:C/I:N/A:N",
                "Version": "V2"
            }
        ],
        "EpssScore": 0.015,
        "ExploitAvailable": "YES",
        "FixAvailable": "YES",
        "Id": "CVE-2020-12345",
        "LastKnownExploitAt": "2020-01-16T00:01:35Z",
        "ReferenceUrls":[
           "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12418",
            "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17563"
        ],
        "RelatedVulnerabilities": ["CVE-2020-12345"],
        "Vendor": {
            "Name": "Alas",
            "Url":"https://alas.aws.amazon.com/ALAS-2020-1337.html",
            "VendorCreatedAt":"2020-01-16T00:01:43Z",
            "VendorSeverity":"Medium",
            "VendorUpdatedAt":"2020-01-16T00:01:43Z"
        },
        "VulnerablePackages": [
            {
                "Architecture": "x86_64",
                "Epoch": "1",
                "FilePath": "/tmp",
                "FixedInVersion": "0.14.0",
                "Name": "openssl",
                "PackageManager": "OS",
                "Release": "16.amzn2.0.3",
                "Remediation": "Update aws-crt to 0.14.0",
                "SourceLayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:id",
                "SourceLayerHash":
 "sha256:c1962c35b63a6ff6ce7df6e042ee82371a605ca9515569edec46ff14f926f001",
                "Version": "1.0.2k"
            }
        ]
    }
]
```

Fluxo de trabalho

O objeto `Workflow` fornece informações sobre o status da investigação de uma descoberta.

Esse campo é destinado aos clientes para uso com ferramentas de remediação, orquestração e emissão de tíquetes. Não se destina a provedores de descoberta.

Você só pode atualizar o campo `Workflow` com `BatchUpdateFindings`. Os clientes também podem atualizá-lo pelo console. Consulte the section called “Definir o status do fluxo de trabalho das descobertas”.

Exemplo

```
"Workflow": {
    "Status": "NEW"
}
```

WorkflowState (Aposentado)

Esse objeto foi retirado e substituído pelo campo `Status` do objeto`Workflow`.

Esse campo fornece o estado do fluxo de trabalho de uma descoberta. Os produtos de descobertas podem fornecer o valor de `NEW` para esse campo. Um produto de descobertas pode fornecer um valor para esse campo se houver um analógico significativo no sistema do produto de descobertas.

Exemplo

```
"WorkflowState": "NEW"
```

Resources

O objeto `Resources` fornece informações sobre os recursos envolvidos em uma descoberta.

Ele contém uma matriz de até 32 objetos de recursos.

Para determinar como os nomes dos recursos são formatados, consulte AWS Sintaxe do Security Finding Format (ASFF).

Para obter exemplos de cada objeto de recurso, selecione na lista a seguir.

Tópicos

- Atributos de recursos
- AwsAmazonMQ
- AwsApiGateway

- AwsAppSync
- AwsAthena
- AwsAutoScaling
- AwsBackup
- AwsCertificateManager
- AwsCloudFormation
- AwsCloudFront
- AwsCloudTrail
- AwsCloudWatch
- AwsCodeBuild
- AwsDms
- AwsDynamoDB
- AwsEc2
- AwsEcr
- AwsEcs
- AwsEfs
- AwsEks
- AwsElasticBeanstalk
- AwsElasticSearch
- AwsElb
- AwsEventBridge
- AwsGuardDuty
- AwsIam
- AwsKinesis
- AwsKms
- AwsLambda
- AwsMsk
- AwsNetworkFirewall
- AwsOpenSearchService
- AwsRds

- AwsRedshift
- AwsRoute53
- AwsS3
- AwsSageMaker
- AwsSecretsManager
- AwsSns
- AwsSqs
- AwsSsm
- AwsStepFunctions
- AwsWaf
- AwsXray
- Container
- Other

Atributos de recursos

Aqui estão as descrições e exemplos do `Resources` objeto no AWS Security Finding Format (ASFF). Para obter mais informações sobre esses campos, consulte Recursos.

ApplicationArn

Identifica o nome do recurso da Amazon (ARN) da aplicação envolvida na descoberta.

Exemplo

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0"
```

ApplicationName

Identifica o nome da aplicação envolvida na descoberta.

Exemplo

```
"ApplicationName": "SampleApp"
```

DataClassification

O campo DataClassification fornece informações sobre dados confidenciais que foram detectados no recurso.

Exemplo

```
"DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
                        }
                    },
                    {
                        "Count": 59,
                        "Type": "EMAIL_ADDRESS",
                        "Occurrences": {
                            "Pages": [
                                {
                                    "PageNumber": 1,
```

```
                            "OffsetRange": {
                                "Start": 1,
                                "End": 100,
                                "StartColumn": 10
                             },
                            "LineRange": {
                                "Start": 1,
                                "End": 100,
                                "StartColumn": 10
                            }
                        }
                    ]
                }
            },
            {
                "Count": 2229,
                "Type": "URL",
                "Occurrences": {
                   "LineRanges": [
                       {
                           "Start": 1,
                           "End": 13
                       }
                   ]
               }
           },
           {
               "Count": 13826,
               "Type": "NameDetection",
               "Occurrences": {
                    "Records": [
                        {
                            "RecordIndex": 1,
                            "JsonPath": "$.ssn.value"
                        }
                    ]
                }
           },
           {
               "Count": 32,
               "Type": "AddressDetection"
           }
       ],
       "TotalCount": 32
```

```
            }
        ],
        "CustomDataIdentifiers": {
            "Detections": [
                {
                    "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                    "Name": "1712be25e7c7f53c731fe464f1c869b8",
                    "Count": 2,
                }
            ],
            "TotalCount": 2
        }
    }
}
```

Detalhes

O campo Details fornece informações adicionais sobre um único recurso usando os objetos apropriados. Cada recurso deve ser fornecido em um objeto de recurso separado no objeto `Resources`.

Observe que, se o tamanho da descoberta exceder o máximo de 240 KB, o objeto `Details` será removido da descoberta. Para descobertas de controle que usam AWS Config regras, você pode visualizar os detalhes do recurso no AWS Config console.

O Security Hub fornece um conjunto de detalhes de recursos disponíveis para seus tipos de recursos compatíveis. Esses detalhes correspondem aos valores do objeto `Type`. Use os tipos fornecidos sempre que possível.

Por exemplo, se o recurso for um bucket do S3, defina o recurso `Type` com `AwsS3Bucket` e forneça os detalhes do recurso no objeto `AwsS3Bucket`.

O objeto `Other` permite fornecer campos e valores personalizados. Use o objeto `Other` nos seguintes casos.

- O tipo de recurso (o valor do recurso `Type`) não tem um objeto correspondente detalhado. Para fornecer detalhes para o recurso, use o objeto `Other`.
- O subcampo do tipo de recurso não inclui todos os campos que você deseja preencher. Nesse caso, use o subcampo do tipo de recurso para preencher os campos disponíveis. Use o subcampo `Other` para preencher os campos que não estão no subcampo específico do tipo.

- O tipo de recurso não é um dos tipos fornecidos. Nesse caso, defina `Resource.Type` como `Other` e use o subcampo `Other` para preencher os detalhes.

Exemplo

```
"Details": {
  "AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IpV4Addresses": ["1.1.1.1"],
    "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
      "HttpProtocolIpv6": "enabled",
      "HttpPutResponseHopLimit": 1,
      "HttpTokens": "optional",
      "InstanceMetadataTags": "disabled"
    },
    "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
    ],
    "SubnetId": "PublicSubnet",
    "Type": "i3.xlarge",
    "VirtualizationType": "hvm",
    "VpcId": "TestVPCIpv6"
  },
  "AwsS3Bucket": {
    "OwnerId": "da4d66eac431652a4d44d490a00500bded52c97d235b7b4752f9f688566fe6de",
    "OwnerName": "acmes3bucketowner"
  },
  "Other": { "LightPen": "blinky", "SerialNo": "1234abcd"}
}
```

Id

O identificador canônico para o tipo de recurso fornecido.

Para AWS recursos identificados pelos Amazon Resource Names (ARNs), esse é o ARN.

Para AWS recursos sem ARNs, esse é o identificador definido pelo AWS serviço que criou o recurso.

Para pessoas que não são AWS recursos, esse é um identificador exclusivo associado ao recurso.

Exemplo

```
"Id": "arn:aws:s3:::example-bucket"
```

Partition

A partição na qual o recurso está localizado. Uma partição é um grupo de Regiões da AWS. Cada uma Conta da AWS tem como escopo uma partição.

As seguintes partições são suportadas:

- `aws` – Regiões da AWS
- `aws-cn`: regiões da China
- `aws-us-gov` – AWS GovCloud (US) Region

Exemplo

```
"Partition": "aws"
```

Região

O código de Região da AWS onde esse recurso está localizado. Para obter uma lista dos códigos das regiões da , consulte Regions and Endpoints.

Exemplo

```
"Region": "us-west-2"
```

ResourceRole

Identifica a função do recurso na descoberta. Um recurso é o alvo da atividade de descoberta ou o ator que realizou a atividade.

Exemplo

```
"ResourceRole": "target"
```

Tags

Você pode adicionar tags de recursos às descobertas que são ingeridas no Security Hub, incluindo descobertas de produtos integrados Serviços da AWS e de terceiros. Você pode marcar recursos compatíveis com a `GetResources` operação da API de AWS Resource Groups marcação. Para ver uma lista dos recursos compatíveis, consulte Serviços que oferecem suporte à API Resource Groups Tagging.

Adicionar tags mostra as tags que estavam associadas a um recurso no momento em que a descoberta foi processada. Você pode incluir o `Tags` atributo somente para recursos que tenham uma tag associada. Se um recurso não tiver uma tag associada, não inclua um atributo `Tags` na descoberta.

A inclusão de tags de recursos nas descobertas elimina a necessidade de criar canais de enriquecimento de dados ou enriquecer manualmente os metadados das descobertas de segurança. Você também pode usar tags para pesquisar ou filtrar descobertas e insights e criar regras de automação.

Para obter informações sobre restrições que se aplicam às tags, consulte Limites e requisitos de nomenclatura de tags.

Você só pode fornecer tags que existam em um AWS recurso nesse campo. Para fornecer dados que não estejam definidos no Formato de descoberta AWS de segurança, use o subcampo de `Other` detalhes.

Exemplo

```
"Tags": {
    "billingCode": "Lotus-1-2-3",
    "needsPatching": "true"
}
```

Tipo

O tipo do recurso para o qual você está fornecendo detalhes.

Sempre que possível, use um dos tipos de recursos fornecidos, como `AwsEc2Instance` ou `AwsS3Bucket`.

Se o tipo de recurso não corresponder a nenhum dos tipos de recurso fornecidos, defina o recurso `Type` como `Other` e use o subcampo de detalhes `Other` para preencher os detalhes.

Os valores suportados estão listados em Recursos.

Exemplo

```
"Type": "AwsS3Bucket"
```

AwsAmazonMQ

A seguir estão exemplos do AWS Security Finding Format (ASFF) para `AwsAmazonMQ` recursos.

AwsAmazonMQBroker

`AwsAmazonMQBroker` fornece informações sobre o agente do Amazon MQ, que é um ambiente de agente de mensagens em execução no Amazon MQ.

O exemplo a seguir mostra o formato do campo `AwsAmazonMQBroker`. Para ver as descrições dos `AwsAmazonMQBroker` atributos, consulte AwsAmazonMQBroker na Referência da AWS Security Hub API.

Exemplo

```
"AwsAmazonMQBroker": {
    "AutoMinorVersionUpgrade": true,
    "BrokerArn": "arn:aws:mq:us-east-1:123456789012:broker:TestBroker:b-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerId": "b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerName": "TestBroker",
    "Configuration": {
        "Id": "c-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "Revision": 1
    },
    "DeploymentMode": "ACTIVE_STANDBY_MULTI_AZ",
    "EncryptionOptions": {
        "UseAwsOwnedKey": true
    },
    "EngineType": "ActiveMQ",
    "EngineVersion": "5.17.2",
    "HostInstanceType": "mq.t2.micro",
    "Logs": {
        "Audit": false,
        "AuditLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/
audit",
        "General": false,
```

```
        "GeneralLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111/general"
    },
    "MaintenanceWindowStartTime": {
        "DayOfWeek": "MONDAY",
        "TimeOfDay": "22:00",
        "TimeZone": "UTC"
    },
    "PubliclyAccessible": true,
    "SecurityGroups": [
        "sg-021345abcdef6789"
    ],
    "StorageType": "efs",
    "SubnetIds": [
        "subnet-1234567890abcdef0",
        "subnet-abcdef01234567890"
    ],
    "Users": [
        {
            "Username": "admin"
        }
    ]
}
```

AwsApiGateway

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsApiGateway` recursos.

AwsApiGatewayRestApi

O objeto `AwsApiGatewayRestApi` contém informações sobre uma API REST na versão 1 do Amazon API Gateway.

O exemplo a seguir é um exemplo de descoberta `AwsApiGatewayRestApi` no AWS Formato do Security Finding (ASFF). Para ver as descrições dos `AwsApiGatewayRestApi` atributos, consulte AwsApiGatewayRestApiDetailsna Referência AWS Security Hub da API.

Exemplo

```
AwsApiGatewayRestApi: {
    "Id": "exampleapi",
    "Name": "Security Hub",
```

```
    "Description": "AWS Security Hub",
    "CreatedDate": "2018-11-18T10:20:05-08:00",
    "Version": "2018-10-26",
    "BinaryMediaTypes" : ["-'*~1*'"],
    "MinimumCompressionSize": 1024,
    "ApiKeySource": "AWS_ACCOUNT_ID",
    "EndpointConfiguration": {
        "Types": [
            "REGIONAL"
        ]
    }
}
```

AwsApiGatewayStage

O objeto `AwsApiGatewayStage` contém informações sobre uma API REST na versão 1 do Amazon API Gateway.

O exemplo a seguir é um exemplo de descoberta `AwsApiGatewayStage` no AWS Formato do Security Finding (ASFF). Para ver as descrições dos `AwsApiGatewayStage` atributos, consulte AwsApiGatewayStageDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsApiGatewayStage": {
    "DeploymentId": "n7hlmf",
    "ClientCertificateId": "a1b2c3",
    "StageName": "Prod",
    "Description" : "Stage Description",
    "CacheClusterEnabled": false,
    "CacheClusterSize" : "1.6",
    "CacheClusterStatus": "NOT_AVAILABLE",
    "MethodSettings": [
        {
            "MetricsEnabled": true,
            "LoggingLevel": "INFO",
            "DataTraceEnabled": false,
            "ThrottlingBurstLimit": 100,
            "ThrottlingRateLimit": 5.0,
            "CachingEnabled": false,
            "CacheTtlInSeconds": 300,
            "CacheDataEncrypted": false,
            "RequireAuthorizationForCacheControl": true,
```

```
            "UnauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER",
            "HttpMethod": "POST",
            "ResourcePath": "/echo"
        }
    ],
    "Variables": {"test": "value"},
    "DocumentationVersion": "2.0",
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "CanarySettings": {
        "PercentTraffic": 0.0,
        "DeploymentId": "ul73s8",
        "StageVariableOverrides" : [
            "String" : "String"
        ],
        "UseStageCache": false
    },
    "TracingEnabled": false,
    "CreatedDate": "2018-07-11T10:55:18-07:00",
    "LastUpdatedDate": "2020-08-26T11:51:04-07:00",
    "WebAclArn" : "arn:aws:waf-regional:us-west-2:111122223333:webacl/
cb606bd8-5b0b-4f0b-830a-dd304e48a822"
}
```

AwsApiGatewayAPI V2

O objeto `AwsApiGatewayV2Api` contém informações sobre uma API REST na versão 1 do Amazon API Gateway.

O exemplo a seguir é um exemplo de descoberta `AwsApiGatewayV2Api` no AWS Formato do Security Finding (ASFF). Para ver as descrições dos `AwsApiGatewayV2Api` atributos, consulte AwsApiGatewayV2 ApiDetails na Referência da AWS Security Hub API.

Exemplo

```
"AwsApiGatewayV2Api": {
    "ApiEndpoint": "https://example.us-west-2.amazonaws.com",
    "ApiId": "a1b2c3d4",
    "ApiKeySelectionExpression": "$request.header.x-api-key",
    "CreatedDate": "2020-03-28T00:32:37Z",
   "Description": "ApiGatewayV2 Api",
   "Version": "string",
    "Name": "my-api",
    "ProtocolType": "HTTP",
    "RouteSelectionExpression": "$request.method $request.path",
   "CorsConfiguration": {
        "AllowOrigins": [ "*" ],
        "AllowCredentials": true,
        "ExposeHeaders": [ "string" ],
        "MaxAge": 3000,
        "AllowMethods": [
          "GET",
          "PUT",
          "POST",
          "DELETE",
          "HEAD"
        ],
        "AllowHeaders": [ "*" ]
    }
}
```

AwsApiGatewayEstágio V2

`AwsApiGatewayV2Stage` contém informações sobre um estágio de versão 2 para o Amazon API Gateway.

O exemplo a seguir é um exemplo de descoberta `AwsApiGatewayV2Stage` no AWS Formato do Security Finding (ASFF). Para ver as descrições dos `AwsApiGatewayV2Stage` atributos, consulte AwsApiGatewayV2 StageDetails na Referência da AWS Security Hub API.

Exemplo

```
"AwsApiGatewayV2Stage": {
    "CreatedDate": "2020-04-08T00:36:05Z",
    "Description" : "ApiGatewayV2",
    "DefaultRouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "DeploymentId": "x1zwyv",
    "LastUpdatedDate": "2020-04-08T00:36:13Z",
    "RouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "StageName": "prod",
    "StageVariables": [
        "function": "my-prod-function"
    ],
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
```

```
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "AutoDeploy": false,
    "LastDeploymentStatusMessage": "Message",
    "ApiGatewayManaged": true,
}
```

AwsAppSync

A seguir estão exemplos do AWS Security Finding Format (ASFF) para `AwsAppSync` recursos.

AwsAppSyncGraphQLApi

`AwsAppSyncGraphQLApi`fornece informações sobre uma API AWS AppSync GraphQL, que é uma construção de alto nível para seu aplicativo.

O exemplo a seguir mostra o formato do campo `AwsAppSyncGraphQLApi`. Para ver as descrições dos `AwsAppSyncGraphQLApi` atributos, consulte AwsAppSyncGraphQlAPI na Referência da AWS Security Hub API.

Exemplo

```
"AwsAppSyncGraphQLApi": {
    "AdditionalAuthenticationProviders": [
    {
     "AuthenticationType": "AWS_LAMBDA",
     "LambdaAuthorizerConfig": {
      "AuthorizerResultTtlInSeconds": 300,
      "AuthorizerUri": "arn:aws:lambda:us-east-1:123456789012:function:mylambdafunc"
     }
    },
    {
     "AuthenticationType": "AWS_IAM"
    }
    ],
    "ApiId": "021345abcdef6789",
    "Arn": "arn:aws:appsync:eu-central-1:123456789012:apis/021345abcdef6789",
    "AuthenticationType": "API_KEY",
    "Id": "021345abcdef6789",
```

```
    "LogConfig": {
     "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/appsync-
graphqlapi-logs-eu-central-1",
     "ExcludeVerboseContent": true,
     "FieldLogLevel": "ALL"
    },
    "Name": "My AppSync App",
    "XrayEnabled": true,
}
```

AwsAthena

A seguir estão exemplos do AWS Security Finding Format (ASFF) para `AwsAthena` recursos.

AwsAthenaWorkGroup

`AwsAthenaWorkGroup` fornece informações sobre um grupo de trabalho do Amazon Athena. Um grupo de trabalho ajuda você a separar usuários, equipes, aplicativos ou workloads. Também ajuda a definir limites no processamento de dados e monitorar os custos.

O exemplo a seguir mostra o formato do campo `AwsAthenaWorkGroup`. Para ver as descrições dos `AwsAthenaWorkGroup` atributos, consulte AwsAthenaWorkGroupna Referência AWS Security Hub da API.

Exemplo

```
"AwsAthenaWorkGroup": {
    "Description": "My workgroup for prod workloads",
    "Name": "MyWorkgroup",
    "WorkgroupConfiguration" {
        "ResultConfiguration": {
            "EncryptionConfiguration": {
                "EncryptionOption": "SSE_KMS",
                "KmsKey": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111"
            }
        }
    },
        "State": "ENABLED"
}
```

AwsAutoScaling

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsAutoScaling` recursos.

AwsAutoScalingAutoScalingGroup

O objeto `AwsAutoScalingAutoScalingGroup` fornece detalhes sobre um grupo de escalabilidade automática.

O exemplo a seguir é um exemplo de descoberta `AwsAutoScalingAutoScalingGroup` no AWS Formato do Security Finding (ASFF). Para ver as descrições dos `AwsAutoScalingAutoScalingGroup` atributos, consulte AwsAutoScalingAutoScalingGroupDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsAutoScalingAutoScalingGroup": {
        "CreatedTime": "2017-10-17T14:47:11Z",
        "HealthCheckGracePeriod": 300,
        "HealthCheckType": "EC2",
        "LaunchConfigurationName": "mylaunchconf",
        "LoadBalancerNames": [],
        "LaunchTemplate": {
            "LaunchTemplateId": "string",
            "LaunchTemplateName": "string",
            "Version": "string"
        },
        "MixedInstancesPolicy": {
            "InstancesDistribution": {
                "OnDemandAllocationStrategy": "prioritized",
                "OnDemandBaseCapacity": number,
                "OnDemandPercentageAboveBaseCapacity": number,
                "SpotAllocationStrategy": "lowest-price",
                "SpotInstancePools": number,
                "SpotMaxPrice": "string"
            },
            "LaunchTemplate": {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "string",
                    "LaunchTemplateName": "string",
                    "Version": "string"
```

```
                },
                "CapacityRebalance": true,
                "Overrides": [
                    {
                       "InstanceType": "string",
                       "WeightedCapacity": "string"
                    }
                ]
            }
        }
    }
}
```

AwsAutoScalingLaunchConfiguration

O objeto fornece detalhes sobre a configuração de uma função do .

Veja a seguir um exemplo de `AwsAutoScalingLaunchConfiguration` descoberta no AWS Security Finding Format (ASFF).

Para ver as descrições dos `AwsAutoScalingLaunchConfiguration` atributos, consulte AwsAutoScalingLaunchConfigurationDetailsna Referência AWS Security Hub da API.

Exemplo

```
AwsAutoScalingLaunchConfiguration: {
    "LaunchConfigurationName": "newtest",
    "ImageId": "ami-058a3739b02263842",
    "KeyName": "55hundredinstance",
    "SecurityGroups": [ "sg-01fce87ad6e019725" ],
    "ClassicLinkVpcSecurityGroups": [],
    "UserData": "...Base64-Encoded user data..."
    "InstanceType": "a1.metal",
    "KernelId": "",
    "RamdiskId": "ari-a51cf9cc",
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/sdh",
            "Ebs": {
                "VolumeSize": 30,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true,
```

```
                "SnapshotId": "snap-ffaa1e69",
                "VirtualName": "ephemeral1"
            }
        },
        {
            "DeviceName": "/dev/sdb",
            "NoDevice": true
        },
        {
            "DeviceName": "/dev/sda1",
            "Ebs": {
                "SnapshotId": "snap-02420cd3d2dea1bc0",
                "VolumeSize": 8,
                "VolumeType": "gp2",
                "DeleteOnTermination": true,
                "Encrypted": false
            }
        },
        {
            "DeviceName": "/dev/sdi",
            "Ebs": {
                "VolumeSize": 20,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true
            }
        },
        {
            "DeviceName": "/dev/sdc",
            "NoDevice": true
        }
    ],
    "InstanceMonitoring": {
        "Enabled": false
    },
    "CreatedTime": 1620842933453,
    "EbsOptimized": false,
    "AssociatePublicIpAddress": true,
    "SpotPrice": "0.045"
}
```

AwsBackup

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsBackup` recursos.

AwsBackupBackupPlan

O objeto `AwsBackupBackupPlan` fornece informações sobre um projeto do AWS Backup . Um plano de AWS Backup backup é uma expressão de política que define quando e como você deseja fazer backup de seus AWS recursos.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsBackupBackupPlan` objeto. Para ver as descrições dos `AwsBackupBackupPlan` atributos, consulte AwsBackupBackupPlannna Referência AWS Security Hub da API.

Exemplo

```
"AwsBackupBackupPlan": {
    "BackupPlan": {
     "AdvancedBackupSettings": [{
      "BackupOptions": {
       "WindowsVSS":"enabled"
      },
      "ResourceType":"EC2"
     }],
     "BackupPlanName": "test",
     "BackupPlanRule": [{
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "DailyBackups",
      "ScheduleExpression": "cron(0 5 ? * * *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
      },
      {
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
```

```
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "Monthly",
      "ScheduleExpression": "cron(0 5 1 * ? *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
     }]
    },
    "BackupPlanArn": "arn:aws:backup:us-east-1:858726136373:backup-
plan:b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "BackupPlanId": "b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "VersionId": "ZDVjNDIzMjItYTZiNS00NzczLTg4YzctNmExMWM2NjZhY2E1"
}
```

AwsBackupBackupVault

O objeto `AwsBackupBackupVault` fornece informações sobre um projeto do AWS Backup . Um cofre AWS Backup de backup é um contêiner que armazena e organiza seus backups.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsBackupBackupVault` objeto. Para ver as descrições dos `AwsBackupBackupVault` atributos, consulte AwsBackupBackupVaultna Referência AWS Security Hub da API.

Exemplo

```
"AwsBackupBackupVault": {
    "AccessPolicy": {
     "Statement": [{
      "Action": [
       "backup:DeleteBackupVault",
       "backup:DeleteBackupVaultAccessPolicy",
       "backup:DeleteRecoveryPoint",
       "backup:StartCopyJob",
       "backup:StartRestoreJob",
       "backup:UpdateRecoveryPointLifecycle"
```

```
      ],
      "Effect": "Deny",
      "Principal": {
       "AWS": "*"
      },
      "Resource": "*"
     }],
     "Version": "2012-10-17"
    },
    "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:aws/efs/
automatic-backup-vault",
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "EncrytionKeyArn": "arn:aws:kms:us-east-1:444455556666:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "Notifications": {
     "BackupVaultEvents": ["BACKUP_JOB_STARTED", "BACKUP_JOB_COMPLETED",
 "COPY_JOB_STARTED"],
     "SNSTopicArn": "arn:aws:sns:us-west-2:111122223333:MyVaultTopic"
    }
}
```

AwsBackupRecoveryPoint

O objeto `AwsBackupRecoveryPoint` fornece informações sobre um backup AWS Backup , também chamado de ponto de recuperação. Um ponto AWS Backup de recuperação representa o conteúdo de um recurso em um horário especificado.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsBackupRecoveryPoint` objeto. Para ver as descrições dos `AwsBackupBackupVault` atributos, consulte AwsBackupRecoveryPointna Referência AWS Security Hub da API.

Exemplo

```
"AwsBackupRecoveryPoint": {
    "BackupSizeInBytes": 0,
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "BackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/efs/
automatic-backup-vault",
    "CalculatedLifecycle": {
     "DeleteAt": "2021-08-30T06:51:58.271Z",
     "MoveToColdStorageAt": "2020-08-10T06:51:58.271Z"
    },
```

```
    "CompletionDate": "2021-07-26T07:21:40.361Z",
    "CreatedBy": {
     "BackupPlanArn": "arn:aws:backup:us-east-1:111122223333:backup-plan:aws/
efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanId": "aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanVersion": "ZGM4YzY5YjktMWYxNC00ZTBmLWE5MjYtZmU5OWNiZmM5ZjIz",
     "BackupRuleId": "2a600c2-42ad-4196-808e-084923ebfd25"
    },
    "CreationDate": "2021-07-26T06:51:58.271Z",
    "EncryptionKeyArn": "arn:aws:kms:us-east-1:111122223333:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "IamRoleArn": "arn:aws:iam::111122223333:role/aws-service-role/
backup.amazonaws.com/AWSServiceRoleForBackup",
    "IsEncrypted": true,
    "LastRestoreTime": "2021-07-26T06:51:58.271Z",
    "Lifecycle": {
     "DeleteAfterDays": 35,
     "MoveToColdStorageAfterDays": 15
    },
    "RecoveryPointArn": "arn:aws:backup:us-east-1:111122223333:recovery-point:151a59e4-
f1d5-4587-a7fd-0774c6e91268",
    "ResourceArn": "arn:aws:elasticfilesystem:us-east-1:858726136373:file-system/
fs-15bd31a1",
    "ResourceType": "EFS",
    "SourceBackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/
efs/automatic-backup-vault",
    "Status": "COMPLETED",
    "StatusMessage": "Failure message",
    "StorageClass": "WARM"
}
```

AwsCertificateManager

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsCertificateManager` recursos.

AwsCertificateManagerCertificate

O objeto `AwsCertificateManagerCertificate` fornece detalhes sobre um certificado AWS Certificate Manager (ACM).

Veja a seguir um exemplo de `AwsCertificateManagerCertificate` descoberta no AWS Security Finding Format (ASFF). Para ver as descrições

dos `AwsCertificateManagerCertificate` atributos, consulte AwsCertificateManagerCertificateDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsCertificateManagerCertificate": {
    "CertificateAuthorityArn": "arn:aws:acm:us-west-2:444455556666:certificate-
authority/example",
    "CreatedAt": "2019-05-24T18:12:02.000Z",
    "DomainName": "example.amazondomains.com",
    "DomainValidationOptions": [
        {
            "DomainName": "example.amazondomains.com",
            "ResourceRecord": {
                "Name": "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                "Type": "CNAME",
                "Value": "_example.acm-validations.aws."
             },
             "ValidationDomain": "example.amazondomains.com",
             "ValidationEmails": [sample_email@sample.com],
             "ValidationMethod": "DNS",
             "ValidationStatus": "SUCCESS"
        }
    ],
    "ExtendedKeyUsages": [
        {
            "Name": "TLS_WEB_SERVER_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.1"
        },
        {
            "Name": "TLS_WEB_CLIENT_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.2"
        }
    ],
    "FailureReason": "",
    "ImportedAt": "2018-08-17T00:13:00.000Z",
    "InUseBy": ["arn:aws:amazondomains:us-west-2:444455556666:loadbalancer/example"],
    "IssuedAt": "2020-04-26T00:41:17.000Z",
    "Issuer": "Amazon",
    "KeyAlgorithm": "RSA-1024",
    "KeyUsages": [
        {
            "Name": "DIGITAL_SIGNATURE",
        },
```

```
        {
            "Name": "KEY_ENCIPHERMENT",
        }
    ],
    "NotAfter": "2021-05-26T12:00:00.000Z",
    "NotBefore": "2020-04-26T00:00:00.000Z",
    "Options": {
        "CertificateTransparencyLoggingPreference": "ENABLED",
    }
    "RenewalEligibility": "ELIGIBLE",
    "RenewalSummary": {
        "DomainValidationOptions": [
            {
                "DomainName": "example.amazondomains.com",
                "ResourceRecord": {
                    "Name":
 "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                    "Type": "CNAME",
                    "Value": "_example.acm-validations.aws.com",
                },
                "ValidationDomain": "example.amazondomains.com",
                "ValidationEmails": ["sample_email@sample.com"],
                "ValidationMethod": "DNS",
                "ValidationStatus": "SUCCESS"
            }
        ],
        "RenewalStatus": "SUCCESS",
        "RenewalStatusReason": "",
        "UpdatedAt": "2020-04-26T00:41:35.000Z",
    },
    "Serial": "02:ac:86:b6:07:2f:0a:61:0e:3a:ac:fd:d9:ab:17:1a",
    "SignatureAlgorithm": "SHA256WITHRSA",
    "Status": "ISSUED",
    "Subject": "CN=example.amazondomains.com",
    "SubjectAlternativeNames": ["example.amazondomains.com"],
    "Type": "AMAZON_ISSUED"
}
```

AwsCloudFormation

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsCloudFormation` recursos.

AwsCloudFormationStack

O objeto `AwsCloudFormationStack` fornece detalhes sobre uma pilha AWS CloudFormation que se aninha como um recurso em um modelo de nível superior.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsCloudFormationStack` objeto. Para ver as descrições dos `AwsCloudFormationStack` atributos, consulte AwsCloudFormationStackDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsCloudFormationStack": {
 "Capabilities": [
  "CAPABILITY_IAM",
  "CAPABILITY_NAMED_IAM"
 ],
 "CreationTime": "2022-02-18T15:31:53.161Z",
 "Description": "AWS CloudFormation Sample",
 "DisableRollback": true,
 "DriftInformation": {
  "StackDriftStatus": "DRIFTED"
 },
 "EnableTerminationProtection": false,
 "LastUpdatedTime": "2022-02-18T15:31:53.161Z",
 "NotificationArns": [
  "arn:aws:sns:us-east-1:978084797471:sample-sns-cfn"
 ],
 "Outputs": [{
  "Description": "URL for newly created LAMP stack",
  "OutputKey": "WebsiteUrl",
  "OutputValue": "http://ec2-44-193-18-241.compute-1.amazonaws.com"
 }],
 "RoleArn": "arn:aws:iam::012345678910:role/exampleRole",
 "StackId": "arn:aws:cloudformation:us-east-1:978084797471:stack/sample-stack/
e5d9f7e0-90cf-11ec-88c6-12ac1f91724b",
 "StackName": "sample-stack",
 "StackStatus": "CREATE_COMPLETE",
 "StackStatusReason": "Success",
 "TimeoutInMinutes": 1
}
```

AwsCloudFront

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsCloudFront` recursos.

AwsCloudFrontDistribution

O `AwsCloudFrontDistribution` objeto fornece detalhes sobre uma configuração de CloudFront distribuição da Amazon.

O exemplo a seguir é um exemplo de descoberta `AwsCloudFrontDistribution` no AWS Formato do Security Finding (ASFF). Para ver as descrições dos `AwsCloudFrontDistribution` atributos, consulte AwsCloudFrontDistributionDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsCloudFrontDistribution": {
    "CacheBehaviors": {
        "Items": [
            {
               "ViewerProtocolPolicy": "https-only"
            }
         ]
    },
    "DefaultCacheBehavior": {
         "ViewerProtocolPolicy": "https-only"
    },
    "DefaultRootObject": "index.html",
    "DomainName": "d2wkuj2w9l34gt.cloudfront.net",
    "Etag": "E37HOT42DHPVYH",
    "LastModifiedTime": "2015-08-31T21:11:29.093Z",
    "Logging": {
         "Bucket": "myawslogbucket.s3.amazonaws.com",
         "Enabled": false,
         "IncludeCookies": false,
         "Prefix": "myawslog/"
     },
     "OriginGroups": {
          "Items": [
              {
                 "FailoverCriteria": {
                     "StatusCodes": {
                          "Items": [
                              200,
```

```
                            301,
                            404
                        ]
                        "Quantity": 3
                    }
                }
            }
        ]
    },
    "Origins": {
        "Items": [
            {
                "CustomOriginConfig": {
                    "HttpPort": 80,
                    "HttpsPort": 443,
                    "OriginKeepaliveTimeout": 60,
                    "OriginProtocolPolicy": "match-viewer",
                    "OriginReadTimeout": 30,
                    "OriginSslProtocols": {
                      "Items": ["SSLv3", "TLSv1"],
                      "Quantity": 2
                    }
                }
            },
        ]
    },
                "DomainName": "my-bucket.s3.amazonaws.com",
                "Id": "my-origin",
                "OriginPath": "/production",
                "S3OriginConfig": {
                    "OriginAccessIdentity": "origin-access-identity/cloudfront/
E2YFS67H6VB6E4"
                }
        ]
    },
    "Status": "Deployed",
    "ViewerCertificate": {
           "AcmCertificateArn": "arn:aws:acm::123456789012:AcmCertificateArn",
           "Certificate": "ASCAJRRE5XYF52TKRY5M4",
           "CertificateSource": "iam",
           "CloudFrontDefaultCertificate": true,
           "IamCertificateId": "ASCAJRRE5XYF52TKRY5M4",
           "MinimumProtocolVersion": "TLSv1.2_2021",
           "SslSupportMethod": "sni-only"
```

```
      },
      "WebAclId": "waf-1234567890"
}
```

AwsCloudTrail

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsCloudTrail` recursos.

AwsCloudTrailTrail

O objeto `AwsCloudTrailTrail` fornece detalhes sobre uma WebACL do AWS CloudTrail .

O exemplo a seguir é um exemplo de descoberta `AwsCloudTrailTrail` no AWS Formato do Security Finding (ASFF). Para ver as descrições dos `AwsCloudTrailTrail` atributos, consulte AwsCloudTrailTrailDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsCloudTrailTrail": {
    "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-
group:CloudTrail/regression:*",
    "CloudWatchLogsRoleArn": "arn:aws:iam::866482105055:role/
CloudTrail_CloudWatchLogs",
    "HasCustomEventSelectors": true,
    "HomeRegion": "us-west-2",
    "IncludeGlobalServiceEvents": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "KmsKeyId": "kmsKeyId",
    "LogFileValidationEnabled": true,
    "Name": "regression-trail",
    "S3BucketName": "cloudtrail-bucket",
    "S3KeyPrefix": "s3KeyPrefix",
    "SnsTopicArn": "arn:aws:sns:us-east-2:123456789012:MyTopic",
    "SnsTopicName": "snsTopicName",
    "TrailArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail"
}
```

AwsCloudWatch

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsCloudWatch` recursos.

AwsCloudWatchAlarm

O `AwsCloudWatchAlarm` objeto fornece detalhes sobre os CloudWatch alarmes da Amazon que observam uma métrica ou realizam uma ação quando um alarme muda de estado.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsCloudWatchAlarm` objeto. Para ver as descrições dos `AwsCloudWatchAlarm` atributos, consulte AwsCloudWatchAlarmDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsCloudWatchAlarm": {
 "ActonsEnabled": true,
 "AlarmActions": [
  "arn:aws:automate:region:ec2:stop",
  "arn:aws:automate:region:ec2:terminate"
 ],
 "AlarmArn": "arn:aws:cloudwatch:us-west-2:012345678910:alarm:sampleAlarm",
 "AlarmConfigurationUpdatedTimestamp": "2022-02-18T15:31:53.161Z",
 "AlarmDescription": "Alarm Example",
 "AlarmName": "Example",
 "ComparisonOperator": "GreaterThanOrEqualToThreshold",
 "DatapointsToAlarm": 1,
 "Dimensions": [{
  "Name": "InstanceId",
  "Value": "i-1234567890abcdef0"
 }],
 "EvaluateLowSampleCountPercentile": "evaluate",
 "EvaluationPeriods": 1,
 "ExtendedStatistic": "p99.9",
 "InsufficientDataActions": [
  "arn:aws:automate:region:ec2:stop"
 ],
 "MetricName": "Sample Metric",
 "Namespace": "YourNamespace",
 "OkActions": [
  "arn:aws:swf:region:account-id:action/actions/AWS_EC2.InstanceId.Stop/1.0"
 ],
 "Period": 1,
 "Statistic": "SampleCount",
 "Threshold": 12.3,
 "ThresholdMetricId": "t1",
 "TreatMissingData": "notBreaching",
```

```
 "Unit": "Kilobytes/Second"
}
```

AwsCodeBuild

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsCodeBuild` recursos.

AwsCodeBuildProject

O objeto `AwsCodeBuildProject` fornece informações sobre um projeto do AWS CodeBuild .

O exemplo a seguir é um exemplo de descoberta `AwsCodeBuildProject` no AWS Formato do Security Finding (ASFF). Para ver as descrições dos `AwsCodeBuildProject` atributos, consulte AwsCodeBuildProjectDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsCodeBuildProject": {
   "Artifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
       }
   ],
   "SecondaryArtifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
       }
```

```
    ],
    "EncryptionKey": "string",
    "Certificate": "string",
    "Environment": {
       "Certificate": "string",
       "EnvironmentVariables": [
            {
                 "Name": "string",
                 "Type": "string",
                 "Value": "string"
            }
       ],
    "ImagePullCredentialsType": "string",
    "PrivilegedMode": boolean,
    "RegistryCredential": {
        "Credential": "string",
        "CredentialProvider": "string"
    },
    "Type": "string"
    },
    "LogsConfig": {
         "CloudWatchLogs": {
              "GroupName": "string",
              "Status": "string",
              "StreamName": "string"
         },
         "S3Logs": {
              "EncryptionDisabled": boolean,
              "Location": "string",
              "Status": "string"
         }
    },
    "Name": "string",
    "ServiceRole": "string",
    "Source": {
         "Type": "string",
         "Location": "string",
         "GitCloneDepth": integer
    },
    "VpcConfig": {
         "VpcId": "string",
         "Subnets": ["string"],
         "SecurityGroupIds": ["string"]
    }
```

```
}
```

AwsDms

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsDms` recursos.

AwsDmsEndpoint

O `AwsDmsEndpoint` objeto fornece informações sobre um endpoint AWS Database Migration Service (AWS DMS). Um endpoint fornece conexão, tipo de armazenamento de dados e informações de localização sobre seu armazenamento de dados.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsDmsEndpoint` objeto. Para ver as descrições dos `AwsDmsEndpoint` atributos, consulte AwsDmsEndpointDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsDmsEndpoint": {
    "CertificateArn": "arn:aws:dms:us-
east-1:123456789012:cert:EXAMPLEIGDURVZGVJQZDPWJ5A7F2YDJVSMTBWFI",
    "DatabaseName": "Test",
    "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EXAMPLEQB3CZY33F7XV253NAJVBNPK6MJQVFVQA",
    "EndpointIdentifier": "target-db",
    "EndpointType": "TARGET",
    "EngineName": "mariadb",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "Port": 3306,
    "ServerName": "target-db.exampletafyu.us-east-1.rds.amazonaws.com",
    "SslMode": "verify-ca",
    "Username": "admin"
}
```

AwsDmsReplicationInstance

O `AwsDmsReplicationInstance` objeto fornece informações sobre uma instância de replicação AWS Database Migration Service (AWS DMS). O DMS usa uma instância de replicação para se conectar ao armazenamento de dados de origem, ler os dados de origem e formatar os dados para consumo pelo armazenamento de dados de destino.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsDmsReplicationInstance` objeto. Para ver as descrições dos `AwsDmsReplicationInstance` atributos, consulte AwsDmsReplicationInstanceDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsDmsReplicationInstance": {
    "AllocatedStorage": 50,
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1b",
    "EngineVersion": "3.5.1",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "MultiAZ": false,
    "PreferredMaintenanceWindow": "wed:08:08-wed:08:38",
    "PubliclyAccessible": true,
    "ReplicationInstanceClass": "dms.c5.xlarge",
    "ReplicationInstanceIdentifier": "second-replication-instance",
    "ReplicationSubnetGroup": {
        "ReplicationSubnetGroupIdentifier": "default-vpc-2344f44f"
    },
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-003a34e205138138b"
        }
    ]
}
```

AwsDmsReplicationTask

O `AwsDmsReplicationTask` objeto fornece informações sobre uma tarefa de replicação AWS Database Migration Service (AWS DMS). Use uma tarefa de replicação do para mover um conjunto de dados do endpoint de origem para o endpoint de destino.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsDmsReplicationInstance` objeto. Para ver as descrições dos `AwsDmsReplicationInstance` atributos, consulte AwsDmsReplicationInstancena Referência AWS Security Hub da API.

Exemplo

```
"AwsDmsReplicationTask": {
    "CdcStartPosition": "2023-08-28T14:26:22",
    "Id": "arn:aws:dms:us-
east-1:123456789012:task:YDYUOHZIXWKQSUCBMUCQCNY44SJW74VJNB5DFWQ",
    "MigrationType": "cdc",
    "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T7V6RFDP23PYQWUL26N3PF5REKML4YOUGIMYJUI",
    "ReplicationTaskIdentifier": "test-task",
    "ReplicationTaskSettings": "{\"Logging\":{\"EnableLogging\":false,
\"EnableLogContext\":false,\"LogComponents\":[{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"TRANSFORMATION\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",
\"Id\":\"SOURCE_UNLOAD\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"IO\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TARGET_LOAD\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"PERFORMANCE\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SOURCE_CAPTURE\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SORTER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"REST_SERVER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id
\":\"VALIDATOR_EXT\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"TARGET_APPLY\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TASK_MANAGER
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TABLES_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"METADATA_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_FACTORY\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMON\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"ADDONS\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"DATA_STRUCTURE
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMUNICATION\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_TRANSFER\"}],\"CloudWatchLogGroup
\":null,\"CloudWatchLogStream\":null},\"StreamBufferSettings\":{\"StreamBufferCount
\":3,\"CtrlStreamBufferSizeInMB\":5,\"StreamBufferSizeInMB\":8},\"ErrorBehavior
\":{\"FailOnNoTablesCaptured\":true,\"ApplyErrorUpdatePolicy\":\"LOG_ERROR\",
\"FailOnTransactionConsistencyBreached\":false,\"RecoverableErrorThrottlingMax\":1800,
\"DataErrorEscalationPolicy\":\"SUSPEND_TABLE\",\"ApplyErrorEscalationCount\":0,
\"RecoverableErrorStopRetryAfterThrottlingMax\":true,\"RecoverableErrorThrottling
\":true,\"ApplyErrorFailOnTruncationDdl\":false,\"DataTruncationErrorPolicy\":
\"LOG_ERROR\",\"ApplyErrorInsertPolicy\":\"LOG_ERROR\",\"EventErrorPolicy\":
\"IGNORE\",\"ApplyErrorEscalationPolicy\":\"LOG_ERROR\",\"RecoverableErrorCount
\":-1,\"DataErrorEscalationCount\":0,\"TableErrorEscalationPolicy\":\"STOP_TASK
\",\"RecoverableErrorInterval\":5,\"ApplyErrorDeletePolicy\":\"IGNORE_RECORD\",
\"TableErrorEscalationCount\":0,\"FullLoadIgnoreConflicts\":true,\"DataErrorPolicy
\":\"LOG_ERROR\",\"TableErrorPolicy\":\"SUSPEND_TABLE\"},\"TTSettings
\":{\"TTS3Settings\":null,\"TTRecordSettings\":null,\"EnableTT\":false},
\"FullLoadSettings\":{\"CommitRate\":10000,\"StopTaskCachedChangesApplied
\":false,\"StopTaskCachedChangesNotApplied\":false,\"MaxFullLoadSubTasks
\":8,\"TransactionConsistencyTimeout\":600,\"CreatePkAfterFullLoad\":false,
```

```
\"TargetTablePrepMode\":\"DO_NOTHING\"},\"TargetMetadata\":{\"ParallelApplyBufferSize
\":0,\"ParallelApplyQueuesPerThread\":0,\"ParallelApplyThreads\":0,\"TargetSchema
\":\"\",\"InlineLobMaxSize\":0,\"ParallelLoadQueuesPerThread\":0,\"SupportLobs
\":true,\"LobChunkSize\":64,\"TaskRecoveryTableEnabled\":false,\"ParallelLoadThreads
\":0,\"LobMaxSize\":0,\"BatchApplyEnabled\":false,\"FullLobMode\":true,
\"LimitedSizeLobMode\":false,\"LoadMaxFileSize\":0,\"ParallelLoadBufferSize\":0},
\"BeforeImageSettings\":null,\"ControlTablesSettings\":{\"historyTimeslotInMinutes
\":5,\"HistoryTimeslotInMinutes\":5,\"StatusTableEnabled\":false,
\"SuspendedTablesTableEnabled\":false,\"HistoryTableEnabled\":false,\"ControlSchema
\":\"\",\"FullLoadExceptionTableEnabled\":false},\"LoopbackPreventionSettings
\":null,\"CharacterSetSettings\":null,\"FailTaskWhenCleanTaskResourceFailed
\":false,\"ChangeProcessingTuning\":{\"StatementCacheSize\":50,\"CommitTimeout
\":1,\"BatchApplyPreserveTransaction\":true,\"BatchApplyTimeoutMin\":1,
\"BatchSplitSize\":0,\"BatchApplyTimeoutMax\":30,\"MinTransactionSize\":1000,
\"MemoryKeepTime\":60,\"BatchApplyMemoryLimit\":500,\"MemoryLimitTotal\":1024},
\"ChangeProcessingDdlHandlingPolicy\":{\"HandleSourceTableDropped\":true,
\"HandleSourceTableTruncated\":true,\"HandleSourceTableAltered\":true},
\"PostProcessingRules\":null}",
    "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:TZPWV2VCXEGHYOKVKRNHAKJ4Q3RUXACNGFGYWRI",
    "TableMappings": "{\"rules\":[{\"rule-type\":\"selection\",\"rule-id\":
\"969761702\",\"rule-name\":\"969761702\",\"object-locator\":{\"schema-name\":\"%table
\",\"table-name\":\"%example\"},\"rule-action\":\"exclude\",\"filters\":[]}]}",
    "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:ABR8LBOQB3CZY33F7XV253NAJVBNPK6MJQVFVQA"
}
```

AwsDynamoDB

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsDynamoDB` recursos.

AwsDynamoDbTable

O objeto `AwsDynamoDbTable` fornece detalhes sobre uma tabela do Amazon DynamoDB.

O exemplo a seguir é um exemplo de descoberta `AwsDynamoDbTable` no AWS Formato do Security Finding (ASFF). Para ver as descrições dos `AwsDynamoDbTable` atributos, consulte AwsDynamoDbTableDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsDynamoDbTable": {
    "AttributeDefinitions": [
        {
```

```
            "AttributeName": "attribute1",
            "AttributeType": "value 1"
        },
        {
            "AttributeName": "attribute2",
            "AttributeType": "value 2"
        },
        {
            "AttributeName": "attribute3",
            "AttributeType": "value 3"
        }
    ],
    "BillingModeSummary": {
        "BillingMode": "PAY_PER_REQUEST",
        "LastUpdateToPayPerRequestDateTime": "2019-12-03T15:23:10.323Z"
    },
    "CreationDateTime": "2019-12-03T15:23:10.248Z",
    "DeletionProtectionEnabled": true,
    "GlobalSecondaryIndexes": [
        {
            "Backfilling": false,
            "IndexArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
index/exampleIndex",
            "IndexName": "standardsControlArnIndex",
            "IndexSizeBytes": 1862513,
            "IndexStatus": "ACTIVE",
            "ItemCount": 20,
            "KeySchema": [
                {
                    "AttributeName": "City",
                    "KeyType": "HASH"
                },
                {
                    "AttributeName": "Date",
                    "KeyType": "RANGE"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
            "ProvisionedThroughput": {
                "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
                "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
```

```
                "NumberOfDecreasesToday": 0,
                "ReadCapacityUnits": 100,
                "WriteCapacityUnits": 50
            },
        }
    ],
    "GlobalTableVersion": "V1",
    "ItemCount": 2705,
    "KeySchema": [
        {
            "AttributeName": "zipcode",
            "KeyType": "HASH"
        }
     ],
     "LatestStreamArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
stream/2019-12-03T23:23:10.248",
     "LatestStreamLabel": "2019-12-03T23:23:10.248",
     "LocalSecondaryIndexes": [
        {
            "IndexArn": "arn:aws:dynamodb:us-east-1:111122223333:table/exampleGroup/
index/exampleId",
            "IndexName": "CITY_DATE_INDEX_NAME",
            "KeySchema": [
                {
                    "AttributeName": "zipcode",
                    "KeyType": "HASH"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
        }
    ],
    "ProvisionedThroughput": {
        "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
        "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
        "NumberOfDecreasesToday": 0,
        "ReadCapacityUnits": 100,
        "WriteCapacityUnits": 50
    },
    "Replicas": [
        {
            "GlobalSecondaryIndexes":[
```

```
                {
                    "IndexName": "CITY_DATE_INDEX_NAME",
                    "ProvisionedThroughputOverride": {
                        "ReadCapacityUnits": 10
                    }
                }
            ],
            "KmsMasterKeyId" : "KmsKeyId"
            "ProvisionedThroughputOverride": {
                "ReadCapacityUnits": 10
            },
            "RegionName": "regionName",
            "ReplicaStatus": "CREATING",
            "ReplicaStatusDescription": "replicaStatusDescription"
        }
    ],
    "RestoreSummary" : {
        "SourceBackupArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
backup/backup1",
        "SourceTableArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable",
        "RestoreDateTime": "2020-06-22T17:40:12.322Z",
        "RestoreInProgress": true
    },
    "SseDescription": {
        "InaccessibleEncryptionDateTime": "2018-01-26T23:50:05.000Z",
        "Status": "ENABLED",
        "SseType": "KMS",
        "KmsMasterKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key1"
    },
    "StreamSpecification" : {
        "StreamEnabled": true,
        "StreamViewType": "NEW_IMAGE"
    },
    "TableId": "example-table-id-1",
    "TableName": "example-table",
    "TableSizeBytes": 1862513,
    "TableStatus": "ACTIVE"
}
```

AwsEc2

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsEc2` recursos.

AwsEc2ClientVpnEndpoint

O `AwsEc2ClientVpnEndpoint` objeto fornece informações sobre um AWS Client VPN endpoint. Um endpoint do Client VPN é o recurso que você cria e configura para habilitar e gerenciar sessões de VPN de clientes. É o ponto de término de todas as sessões da VPN do cliente.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEc2ClientVpnEndpoint` objeto. Para ver as descrições dos `AwsEc2ClientVpnEndpoint` atributos, consulte AwsEc2 ClientVpnEndpointDetails na Referência AWS Security Hub da API.

Exemplo

```
"AwsEc2ClientVpnEndpoint": {
    "AuthenticationOptions": [
        {
            "MutualAuthentication": {
                "ClientRootCertificateChainArn": "arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            },
            "Type": "certificate-authentication"
        }
    ],
    "ClientCidrBlock": "10.0.0.0/22",
    "ClientConnectOptions": {
        "Enabled": false
    },
    "ClientLoginBannerOptions": {
        "Enabled": false
    },
    "ClientVpnEndpointId": "cvpn-endpoint-00c5d11fc4729f2a5",
    "ConnectionLogOptions": {
        "Enabled": false
    },
    "Description": "test",
    "DnsServer": ["10.0.0.0"],
    "ServerCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "SecurityGroupIdSet": [
        "sg-0f7a177b82b443691"
    ],
    "SelfServicePortalUrl": "https://self-service.clientvpn.amazonaws.com/endpoints/
cvpn-endpoint-00c5d11fc4729f2a5",
    "SessionTimeoutHours": 24,
```

```
    "SplitTunnel": false,
    "TransportProtocol": "udp",
    "VpcId": "vpc-1a2b3c4d5e6f1a2b3",
    "VpnPort": 443
}
```

AwsEc2Eip

O objeto `AwsEc2Eip` fornece informações sobre um endereço IP elástico.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEc2Eip` objeto. Para ver as descrições dos `AwsEc2Eip` atributos, consulte AwsEc2 EipDetails na Referência AWS Security Hub da API.

Exemplo

```
"AwsEc2Eip": {
    "InstanceId": "instance1",
    "PublicIp": "192.0.2.04",
    "AllocationId": "eipalloc-example-id-1",
    "AssociationId": "eipassoc-example-id-1",
    "Domain": "vpc",
    "PublicIpv4Pool": "anycompany",
    "NetworkBorderGroup": "eu-central-1",
    "NetworkInterfaceId": "eni-example-id-1",
    "NetworkInterfaceOwnerId": "777788889999",
    "PrivateIpAddress": "192.0.2.03"
}
```

AwsEc2Instance

O objeto `AwsEc2Instance` fornece detalhes sobre uma instância do Amazon EC2.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEc2Instance` objeto. Para ver as descrições dos `AwsEc2Instance` atributos, consulte AwsEc2 InstanceDetails na Referência AWS Security Hub da API.

Exemplo

```
"AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
    "ImageId": "ami-1234",
    "IpV4Addresses": [ "1.1.1.1" ],
```

```
    "IpV6Addresses": [ "2001:db8:1234:1a2b::123" ],
    "KeyName": "my_keypair",
    "LaunchedAt": "2018-05-08T16:46:19.000Z",
    "MetadataOptions": {
     "HttpEndpoint": "enabled",
     "HttpProtocolIpv6": "enabled",
     "HttpPutResponseHopLimit": 1,
     "HttpTokens": "optional",
     "InstanceMetadataTags": "disabled",
    },
    "Monitoring": {
     "State": "disabled"
    },
    "NetworkInterfaces": [
      {
         "NetworkInterfaceId": "eni-e5aa89a3"
      }
    ],
    "SubnetId": "subnet-123",
    "Type": "i3.xlarge",
    "VpcId": "vpc-123"
}
```

AwsEc2LaunchTemplate

O objeto `AwsEc2LaunchTemplate` contém detalhes sobre um modelo de lançamento do Amazon Elastic Compute Cloud que especifica as informações de configuração da instância.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEc2LaunchTemplate` objeto. Para ver as descrições dos `AwsEc2LaunchTemplate` atributos, consulte AwsEc2 LaunchTemplateDetails na Referência AWS Security Hub da API.

Exemplo

```
"AwsEc2LaunchTemplate": {
    "DefaultVersionNumber": "1",
    "ElasticGpuSpecifications": ["string"],
    "ElasticInferenceAccelerators": ["string"],
    "Id": "lt-0a16e9802800bdd85",
    "ImageId": "ami-0d5eff06f840b45e9",
    "LatestVersionNumber": "1",
    "LaunchTemplateData": {
     "BlockDeviceMappings": [{
```

```
      "DeviceName": "/dev/xvda",
      "Ebs": {
       "DeleteonTermination": true,
       "Encrypted": true,
       "SnapshotId": "snap-01047646ec075f543",
       "VolumeSize": 8,
       "VolumeType:" "gp2"
      }
     }],
     "MetadataOptions": {
      "HttpTokens": "enabled",
      "HttpPutResponseHopLimit" : 1
     },
     "Monitoring": {
      "Enabled": true,
     "NetworkInterfaces": [{
      "AssociatePublicIpAddress" : true,
     }],
    "LaunchTemplateName": "string",
    "LicenseSpecifications": ["string"],
    "SecurityGroupIds": ["sg-01fce87ad6e019725"],
    "SecurityGroups": ["string"],
    "TagSpecifications": ["string"]
}
```

AwsEc2NetworkAcl

O objeto `AwsEc2NetworkAcl` contém detalhes sobre uma lista de controle de acesso (ACL) da rede do Amazon EC2.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEc2NetworkAcl` objeto. Para ver as descrições dos `AwsEc2NetworkAcl` atributos, consulte AwsEc2 NetworkAclDetails na Referência AWS Security Hub da API.

Exemplo

```
"AwsEc2NetworkAcl": {
    "IsDefault": false,
    "NetworkAclId": "acl-1234567890abcdef0",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234abcd",
    "Associations": [{
        "NetworkAclAssociationId": "aclassoc-abcd1234",
```

```
        "NetworkAclId": "acl-021345abcdef6789",
        "SubnetId": "subnet-abcd1234"
    }],
    "Entries": [{
        "CidrBlock": "10.24.34.0/23",
        "Egress": true,
        "IcmpTypeCode": {
            "Code": 10,
            "Type": 30
        },
        "Ipv6CidrBlock": "2001:DB8::/32",
        "PortRange": {
            "From": 20,
            "To": 40
        },
        "Protocol": "tcp",
        "RuleAction": "allow",
        "RuleNumber": 100
    }]
}
```

AwsEc2NetworkInterface

O objeto `AwsEc2NetworkInterface` fornece informações sobre uma interface de rede do Amazon EC2.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEc2NetworkInterface` objeto. Para ver as descrições dos `AwsEc2NetworkInterface` atributos, consulte AwsEc2 NetworkInterfaceDetails na Referência AWS Security Hub da API.

Exemplo

```
"AwsEc2NetworkInterface": {
    "Attachment": {
        "AttachTime": "2019-01-01T03:03:21Z",
        "AttachmentId": "eni-attach-43348162",
        "DeleteOnTermination": true,
        "DeviceIndex": 123,
        "InstanceId": "i-1234567890abcdef0",
        "InstanceOwnerId": "123456789012",
        "Status": 'ATTACHED'
    },
    "SecurityGroups": [
```

```
        {
            "GroupName": "my-security-group",
            "GroupId": "sg-903004f8"
        },
    ],
    "NetworkInterfaceId": 'eni-686ea200',
    "SourceDestCheck": false
}
```

AwsEc2RouteTable

O objeto `AwsEc2RouteTable` fornece informações sobre uma tabela de rotas do Amazon EC2.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEc2RouteTable` objeto. Para ver as descrições dos `AwsEc2RouteTable` atributos, consulte AwsEc2 RouteTableDetails na Referência AWS Security Hub da API.

Exemplo

```
"AwsEc2RouteTable": {
    "AssociationSet": [{
     "AssociationSet": {
      "State": "associated"
        },
     "Main": true,
     "RouteTableAssociationId": "rtbassoc-08e706c45de9f7512",
     "RouteTableId": "rtb-0a59bde9cf2548e34",
    }],
    "PropogatingVgwSet": [],
    "RouteTableId": "rtb-0a59bde9cf2548e34",
    "RouteSet": [
     {
      "DestinationCidrBlock": "10.24.34.0/23",
      "GatewayId": "local",
      "Origin": "CreateRouteTable",
      "State": "active"
     },
     {
      "DestinationCidrBlock": "10.24.34.0/24",
      "GatewayId": "igw-0242c2d7d513fc5d3",
      "Origin": "CreateRoute",
      "State": "active"
     }
```

```
    ],
    "VpcId": "vpc-0c250a5c33f51d456"
}
```

AwsEc2SecurityGroup

O objeto `AwsEc2SecurityGroup` descreve um grupo de segurança do Amazon EC2.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEc2SecurityGroup` objeto. Para ver as descrições dos `AwsEc2SecurityGroup` atributos, consulte AwsEc2 SecurityGroupDetails na Referência AWS Security Hub da API.

Exemplo

```
"AwsEc2SecurityGroup": {
    "GroupName": "MySecurityGroup",
    "GroupId": "sg-903004f8",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1a2b3c4d",
    "IpPermissions": [
        {
            "IpProtocol": "-1",
            "IpRanges": [],
            "UserIdGroupPairs": [
                {
                    "UserId": "123456789012",
                    "GroupId": "sg-903004f8"
                }
            ],
            "PrefixListIds": [
                {"PrefixListId": "pl-63a5400a"}
            ]
        },
        {
            "PrefixListIds": [],
            "FromPort": 22,
            "IpRanges": [
                {
                    "CidrIp": "203.0.113.0/24"
                }
            ],
            "ToPort": 22,
            "IpProtocol": "tcp",
```

```
            "UserIdGroupPairs": []
        }
    ]
}
```

AwsEc2Subnet

O objeto `AwsEc2Subnet` fornece informações sobre uma tabela de rotas do Amazon EC2.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEc2Subnet` objeto. Para ver as descrições dos `AwsEc2Subnet` atributos, consulte AwsEc2 SubnetDetails na Referência AWS Security Hub da API.

Exemplo

```
AwsEc2Subnet: {
    "AssignIpv6AddressOnCreation": false,
    "AvailabilityZone": "us-west-2c",
    "AvailabilityZoneId": "usw2-az3",
    "AvailableIpAddressCount": 8185,
    "CidrBlock": "10.0.0.0/24",
    "DefaultForAz": false,
    "MapPublicIpOnLaunch": false,
    "OwnerId": "123456789012",
    "State": "available",
    "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/subnet-d5436c93",
    "SubnetId": "subnet-d5436c93",
    "VpcId": "vpc-153ade70",
    "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "subnet-cidr-assoc-EXAMPLE",
        "Ipv6CidrBlock": "2001:DB8::/32",
        "CidrBlockState": "associated"
   }]
}
```

AwsEc2TransitGateway

O objeto `AwsEc2TransitGateway` fornece detalhes sobre o gateway de trânsito do Amazon EC2 que interconecta as nuvens privadas virtuais (VPCs) e as redes on-premises.

Veja a seguir um exemplo de `AwsEc2TransitGateway` descoberta no AWS Security Finding Format (ASFF). Para ver as descrições dos `AwsEc2TransitGateway` atributos, consulte AwsEc2 TransitGatewayDetails na Referência AWS Security Hub da API.

Exemplo

```
"AwsEc2TransitGateway": {
 "AmazonSideAsn": 65000,
 "AssociationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "AutoAcceptSharedAttachments": "disable",
 "DefaultRouteTableAssociation": "enable",
 "DefaultRouteTablePropagation": "enable",
 "Description": "sample transit gateway",
 "DnsSupport": "enable",
 "Id": "tgw-042ae6bf7a5c126c3",
 "MulticastSupport": "disable",
 "PropagationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "TransitGatewayCidrBlocks": ["10.0.0.0/16"],
 "VpnEcmpSupport": "enable"
}
```

AwsEc2Volume

O objeto `AwsEc2Volume` fornece detalhes sobre uma conexão VPN do Amazon EC2.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEc2Volume` objeto. Para ver as descrições dos `AwsEc2Volume` atributos, consulte AwsEc2 VolumeDetails na Referência AWS Security Hub da API.

Exemplo

```
"AwsEc2Volume": {
    "Attachments": [
      {
        "AttachTime": "2017-10-17T14:47:11Z",
        "DeleteOnTermination": true,
        "InstanceId": "i-123abc456def789g",
        "Status": "attached"
      }
     ],
    "CreateTime": "2020-02-24T15:54:30Z",
    "Encrypted": true,
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "Size": 80,
    "SnapshotId": "",
    "Status": "available"
```

```
}
```

AwsEc2Vpc

O objeto `AwsEc2Vpc` fornece detalhes sobre uma conexão VPN do Amazon EC2.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEc2Vpc` objeto. Para ver as descrições dos `AwsEc2Vpc` atributos, consulte AwsEc2 VpcDetails na Referência AWS Security Hub da API.

Exemplo

```
"AwsEc2Vpc": {
    "CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlock": "192.0.2.0/24",
            "CidrBlockState": "associated"
        }
    ],
    "DhcpOptionsId": "dopt-4e42ce28",
    "Ipv6CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlockState": "associated",
            "Ipv6CidrBlock": "192.0.2.0/24"
       }

    ],
    "State": "available"
}
```

AwsEc2VpcEndpointService

O objeto `AwsEc2VpcEndpointService` contém detalhes sobre a configuração do serviço de um endpoint da VPC.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEc2VpcEndpointService` objeto. Para ver as descrições dos `AwsEc2VpcEndpointService` atributos, consulte AwsEc2 VpcEndpointServiceDetails na Referência AWS Security Hub da API.

Exemplo

```
"AwsEc2VpcEndpointService": {
    "ServiceType": [
      {
        "ServiceType": "Interface"
      }
    ],
    "ServiceId": "vpce-svc-example1",
    "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example1",
    "ServiceState": "Available",
    "AvailabilityZones": [
      "us-east-1"
    ],
    "AcceptanceRequired": true,
    "ManagesVpcEndpoints": false,
    "NetworkLoadBalancerArns": [
      "arn:aws:elasticloadbalancing:us-east-1:444455556666:loadbalancer/net/my-network-
load-balancer/example1"
    ],
    "GatewayLoadBalancerArns": [],
    "BaseEndpointDnsNames": [
      "vpce-svc-04eec859668b51c34.us-east-1.vpce.amazonaws.com"
    ],
    "PrivateDnsName": "my-private-dns"
}
```

AwsEc2VpcPeeringConnection

O objeto `AwsEc2VpcPeeringConnection` fornece detalhes sobre a conexão de rede entre duas VPCs.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEc2VpcPeeringConnection` objeto. Para ver as descrições dos `AwsEc2VpcPeeringConnection` atributos, consulte AwsEc2 VpcPeeringConnectionDetails na Referência AWS Security Hub da API.

Exemplo

```
"AwsEc2VpcPeeringConnection": {
 "AccepterVpcInfo": {
  "CidrBlock": "10.0.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "10.0.0.0/28"
```

```
  }],
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
   "AllowDnsResolutionFromRemoteVpc": true,
   "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
   "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
 },
 "ExpirationTime": "2022-02-18T15:31:53.161Z",
 "RequesterVpcInfo": {
  "CidrBlock": "192.168.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "192.168.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
   "AllowDnsResolutionFromRemoteVpc": true,
   "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
   "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
 },
 "Status": {
  "Code": "initiating-request",
  "Message": "Active"
 },
 "VpcPeeringConnectionId": "pcx-1a2b3c4d"
}
```

AwsEc2VpnConnection

O objeto `AwsEc2VpnConnection` fornece detalhes sobre uma conexão VPN do Amazon EC2.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEc2VpnConnection` objeto. Para ver as descrições dos `AwsEc2VpnConnection` atributos, consulte AwsEc2 VpnConnectionDetails na Referência AWS Security Hub da API.

Exemplo

```
"AwsEc2VpnConnection": {
    "VpnConnectionId": "vpn-205e4f41",
    "State": "available",
    "CustomerGatewayConfiguration": "",
    "CustomerGatewayId": "cgw-5699703f",
    "Type": "ipsec.1",
    "VpnGatewayId": "vgw-2ccb2245",
    "Category": "VPN"
    "TransitGatewayId": "tgw-09b6f3a659e2b5elf",
    "VgwTelemetry": [
        {
            "OutsideIpAddress": "92.0.2.11",
            "Status": "DOWN",
            "LastStatusChange": "2016-11-11T23:09:32.000Z",
            "StatusMessage": "IPSEC IS DOWN",
            "AcceptedRouteCount": 0
        },
        {
            "OutsideIpAddress": "92.0.2.12",
            "Status": "DOWN",
            "LastStatusChange": "2016-11-11T23:10:51.000Z",
            "StatusMessage": "IPSEC IS DOWN",
            "AcceptedRouteCount": 0
        }
    ],
    "Routes": [{
        "DestinationCidrBlock": "10.24.34.0/24",
        "State": "available"
   }],
    "Options": {
        "StaticRoutesOnly": true
        "TunnelOptions": [{
            "DpdTimeoutSeconds": 30,
            "IkeVersions": ["ikev1", "ikev2"],
            "Phase1DhGroupNumbers": [14, 15, 16, 17, 18},
            "Phase1EncryptionAlgorithms": ["AES128", "AES256"],
            "Phase1IntegrityAlgorithms": ["SHA1", "SHA2-256"],
```

```
            "Phase1LifetimeSeconds": 28800,
            "Phase2DhGroupNumbers": [14, 15, 16, 17, 18],
            "Phase2EncryptionAlgorithms": ["AES128", "AES256"],
            "Phase2IntegrityAlgorithms": ["SHA1", "SHA2-256"],
            "Phase2LifetimeSeconds": 28800,
            "PreSharedKey": "RltXC3REhTw1RAdiM2s1uMfkkSDLyGJoe1QEWeGxqkQ=",
            "RekeyFuzzPercentage": 100,
            "RekeyMarginTimeSeconds": 540,
            "ReplayWindowSize": 1024,
            "TunnelInsideCidr": "10.24.34.0/23"
        }]
   }
}
```

AwsEcr

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsEcr` recursos.

AwsEcrContainerImage

O objeto `AwsEcrContainerImage` fornece informações sobre uma tabela de rotas do Amazon EC2.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEcrContainerImage` objeto. Para ver as descrições dos `AwsEcrContainerImage` atributos, consulte AwsEcrContainerImageDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsEcrContainerImage": {
    "RegistryId": "123456789012",
    "RepositoryName": "repository-name",
    "Architecture": "amd64"
    "ImageDigest":
 "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
    "ImageTags": ["00000000-0000-0000-0000-000000000000"],
    "ImagePublishedAt": "2019-10-01T20:06:12Z"
}
```

AwsEcrRepository

O objeto `AwsEcrRepository` fornece informações sobre um repositório do Amazon Elastic Container Registry.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEcrRepository` objeto. Para ver as descrições dos `AwsEcrRepository` atributos, consulte AwsEcrRepositoryDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsEcrRepository": {
    "LifecyclePolicy": {
        "RegistryId": "123456789012",
    },
    "RepositoryName": "sample-repo",
    "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
    "ImageScanningConfiguration": {
        "ScanOnPush": true
    },
    "ImageTagMutability": "IMMUTABLE"
}
```

AwsEcs

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsEcs` recursos.

AwsEcsCluster

O objeto `AwsEcsCluster` fornece detalhes sobre um cluster do Amazon Elastic Container Service.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEcsCluster` objeto. Para ver as descrições dos `AwsEcsCluster` atributos, consulte AwsEcsClusterDetailsna Referência AWS Security Hub da API.

Exemplo

```
    "AwsEcsCluster": {
        "CapacityProviders": [],
        "ClusterSettings": [
            {
                "Name": "containerInsights",
                "Value": "enabled"
            }
        ],
        "Configuration": {
            "ExecuteCommandConfiguration": {
                "KmsKeyId": "kmsKeyId",
```

```
                "LogConfiguration": {
                    "CloudWatchEncryptionEnabled": true,
                    "CloudWatchLogGroupName": "cloudWatchLogGroupName",
                    "S3BucketName": "s3BucketName",
                    "S3EncryptionEnabled": true,
                    "S3KeyPrefix": "s3KeyPrefix"
                },
                "Logging": "DEFAULT"
            }
        }
        "DefaultCapacityProviderStrategy": [
            {
                "Base": 0,
                "CapacityProvider": "capacityProvider",
                "Weight": 1
            }
        ]
    }
```

AwsEcsContainer

O objeto `AwsEcsContainer` contém detalhes sobre um contêiner do Amazon ECS.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEcsContainer` objeto. Para ver as descrições dos `AwsEcsContainer` atributos, consulte AwsEcsContainerDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsEcsContainer": {
    "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
    "MountPoints": [{
        "ContainerPath": "/mnt/etc",
        "SourceVolume": "vol-03909e9"
    }],
    "Name": "knote",
    "Privileged": true
}
```

AwsEcsService

O objeto `AwsEcsService` fornece detalhes sobre um cluster do Amazon Elastic Container Service.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEcsService` objeto. Para ver as descrições dos `AwsEcsService` atributos, consulte AwsEcsServiceDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsEcsService": {
    "CapacityProviderStrategy": [
        {
            "Base": 12,
            "CapacityProvider": "",
            "Weight": ""
        }
    ],
    "Cluster": "arn:aws:ecs:us-east-1:111122223333:cluster/example-ecs-cluster",
    "DeploymentConfiguration": {
        "DeploymentCircuitBreaker": {
            "Enable": false,
            "Rollback": false
        },
        "MaximumPercent": 200,
        "MinimumHealthyPercent": 100
    },
    "DeploymentController": "",
    "DesiredCount": 1,
    "EnableEcsManagedTags": false,
    "EnableExecuteCommand": false,
    "HealthCheckGracePeriodSeconds": 1,
    "LaunchType": "FARGATE",
    "LoadBalancers": [
        {
            "ContainerName": "",
            "ContainerPort": 23,
            "LoadBalancerName": "",
            "TargetGroupArn": ""
        }
    ],
    "Name": "sample-app-service",
    "NetworkConfiguration": {
        "AwsVpcConfiguration": {
            "Subnets": [
                "Subnet-example1",
                "Subnet-example2"
```

```
            ],
        "SecurityGroups": [
                "Sg-0ce48e9a6e5b457f5"
        ],
        "AssignPublicIp": "ENABLED"
        }
    },
    "PlacementConstraints": [
        {
            "Expression": "",
            "Type": ""
        }
    ],
    "PlacementStrategies": [
        {
            "Field": "",
            "Type": ""
        }
    ],
    "PlatformVersion": "LATEST",
    "PropagateTags": "",
    "Role": "arn:aws:iam::111122223333:role/aws-servicerole/ecs.amazonaws.com/
ServiceRoleForECS",
    "SchedulingStrategy": "REPLICA",
    "ServiceName": "sample-app-service",
    "ServiceArn": "arn:aws:ecs:us-east-1:111122223333:service/example-ecs-cluster/
sample-app-service",
    "ServiceRegistries": [
        {
            "ContainerName": "",
            "ContainerPort": 1212,
            "Port": 1221,
            "RegistryArn": ""
        }
    ],
    "TaskDefinition": "arn:aws:ecs:us-east-1:111122223333:task-definition/example-
taskdef:1"
}
```

AwsEcsTask

O objeto `AwsEcsTask` fornece detalhes sobre uma tabela do Amazon DynamoDB.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEcsTask` objeto. Para ver as descrições dos `AwsEcsTask` atributos, consulte AwsEcsTaskna Referência AWS Security Hub da API.

Exemplo

```
"AwsEcsTask": {
 "ClusterArn": "arn:aws:ecs:us-west-2:123456789012:task/MyCluster/1234567890123456789",
 "CreatedAt": "1557134011644",
 "Group": "service:fargate-service",
 "StartedAt": "1557134011644",
 "StartedBy": "ecs-svc/1234567890123456789",
 "TaskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-definition/sample-
fargate:2",
 "Version": 3,
 "Volumes": [{
  "Name": "string",
  "Host": {
   "SourcePath": "string"
  }
 }],
 "Containers": {
  "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "MountPoints": [{
   "ContainerPath": "/mnt/etc",
   "SourceVolume": "vol-03909e9"
  }],
  "Name": "knote",
  "Privileged": true
 }
}
```

AwsEcsTaskDefinition

O objeto `AwsEcsTaskDefinition` contém detalhes sobre a definição de uma tarefa. O recurso AWS::ECS::TaskDefinition descreve as definições de contêiner e volume de uma tarefa do Amazon Elastic Container Service (Amazon ECS).

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEcsTaskDefinition` objeto. Para ver as descrições dos `AwsEcsTaskDefinition` atributos, consulte AwsEcsTaskDefinitionDetailsna Referência AWS Security Hub da API.

Exemplo

```
    "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [
            {
                "Command": ['ruby', 'hi.rb'],
                "Cpu":128,
                "Essential": true,
                "HealthCheck": {
                    "Command": ["CMD-SHELL", "curl -f http://localhost/ || exit 1"],
                    "Interval": 10,
                    "Retries": 3,
                    "StartPeriod": 5,
                    "Timeout": 20
                },
                "Image": "tongueroo/sinatra:latest",
                "Interactive": true,
                "Links": [],
                "LogConfiguration": {
                    "LogDriver": "awslogs",
                    "Options": {
                        "awslogs-group": "/ecs/sinatra-hi",
                        "awslogs-region": "ap-southeast-1",
                        "awslogs-stream-prefix": "ecs"
                    },
                    "SecretOptions": []

                },
                "MemoryReservation": 128,
                "Name": "web",
                "PortMappings": [
                    {
                        "ContainerPort": 4567,
                        "HostPort":4567,
                        "Protocol": "tcp"
                    }
                ],
                "Privileged": true,
                "StartTimeout": 10,
                "StopTimeout": 100,
            }
        ],
        "Family": "sinatra-hi",
        "NetworkMode": "host",
```

```
        "RequiresCompatibilities": ["EC2"],
        "Status": "ACTIVE",
        "TaskRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
    }
```

AwsEfs

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsEfs` recursos.

AwsEfsAccessPoint

O objeto `AwsEfsAccessPoint` fornece detalhes sobre os arquivos armazenados no Amazon Elastic File System.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEfsAccessPoint` objeto. Para ver as descrições dos `AwsEfsAccessPoint` atributos, consulte AwsEfsAccessPointDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsEfsAccessPoint": {
 "AccessPointId": "fsap-05c4c0e79ba0b118a",
 "Arn": "arn:aws:elasticfilesystem:us-east-1:863155670886:access-point/
fsap-05c4c0e79ba0b118a",
 "ClientToken": "AccessPointCompliant-ASk06ZZSXsEp",
 "FileSystemId": "fs-0f8137f731cb32146",
 "PosixUser": {
  "Gid": "1000",
  "SecondaryGids": ["0", "4294967295"],
  "Uid": "1234"
 },
 "RootDirectory": {
  "CreationInfo": {
   "OwnerGid": "1000",
   "OwnerUid": "1234",
   "Permissions": "777"
  },
  "Path": "/tmp/example"
 }
}
```

AwsEks

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsEks` recursos.

AwsEksCluster

O objeto `AwsEksCluster` fornece detalhes sobre uma tabela do cluster Amazon EKS.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEksCluster` objeto. Para ver as descrições dos `AwsEksCluster` atributos, consulte AwsEksClusterDetailsna Referência AWS Security Hub da API.

Exemplo

```
{
  "AwsEksCluster": {
    "Name": "example",
    "Arn": "arn:aws:eks:us-west-2:222222222222:cluster/example",
    "CreatedAt": 1565804921.901,
    "Version": "1.12",
    "RoleArn": "arn:aws:iam::222222222222:role/example-cluster-
ServiceRole-1XWBQWYSFRE2Q",
    "ResourcesVpcConfig": {
      "EndpointPublicAccess": false,
      "SubnetIds": [
        "subnet-021345abcdef6789",
        "subnet-abcdef01234567890",
        "subnet-1234567890abcdef0"
      ],
      "SecurityGroupIds": [
        "sg-abcdef01234567890"
      ]
    },
    "Logging": {
      "ClusterLogging": [
        {
          "Types": [
            "api",
            "audit",
            "authenticator",
            "controllerManager",
            "scheduler"
          ],
          "Enabled": true
```

```
        }
      ]
    },
    "Status": "CREATING",
    "CertificateAuthorityData": {},
  }
}
```

AwsElasticBeanstalk

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsElasticBeanstalk` recursos.

AwsElasticBeanstalkEnvironment

O objeto `AwsElasticBeanstalkEnvironment` contém detalhes sobre um ambiente AWS Elastic Beanstalk .

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsElasticBeanstalkEnvironment` objeto. Para ver as descrições dos `AwsElasticBeanstalkEnvironment` atributos, consulte AwsElasticBeanstalkEnvironmentDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsElasticBeanstalkEnvironment": {
    "ApplicationName": "MyApplication",
    "Cname": "myexampleapp-env.devo-2.elasticbeanstalk-internal.com",
    "DateCreated": "2021-04-30T01:38:01.090Z",
    "DateUpdated": "2021-04-30T01:38:01.090Z",
    "Description": "Example description of my awesome application",
    "EndpointUrl": "eb-dv-e-p-AWSEBLoa-abcdef01234567890-021345abcdef6789.us-
east-1.elb.amazonaws.com",
    "EnvironmentArn": "arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/
MyApplication/myapplication-env",
    "EnvironmentId": "e-abcd1234",
    "EnvironmentLinks": [
        {
            "EnvironmentName": "myexampleapp-env",
            "LinkName": "myapplicationLink"
        }
    ],
    "EnvironmentName": "myapplication-env",
```

```
    "OptionSettings": [
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSize",
            "Value": "100"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "Timeout",
            "Value": "600"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSizeType",
            "Value": "Percentage"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "IgnoreHealthCheck",
            "Value": "false"
        },
        {
            "Namespace": "aws:elasticbeanstalk:application",
            "OptionName": "Application Healthcheck URL",
            "Value": "TCP:80"
        }
    ],
    "PlatformArn": "arn:aws:elasticbeanstalk:us-east-1::platform/Tomcat 8 with Java 8
 running on 64bit Amazon Linux/2.7.7",
    "SolutionStackName": "64bit Amazon Linux 2017.09 v2.7.7 running Tomcat 8 Java 8",
    "Status": "Ready",
    "Tier": {
        "Name": "WebServer"
       "Type": "Standard"
       "Version": "1.0"
    },
    "VersionLabel": "Sample Application"
}
```

AwsElasticSearch

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsElasticSearch` recursos.

AwsElasticSearchDomain

O `AwsElasticSearchDomain` objeto fornece detalhes sobre um domínio do Amazon OpenSearch Service.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsElasticSearchDomain` objeto. Para ver as descrições dos `AwsElasticSearchDomain` atributos, consulte AwsElasticSearchDomainDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsElasticSearchDomain": {
    "AccessPolicies": "string",
    "DomainStatus": {
           "DomainId": "string",
           "DomainName": "string",
           "Endpoint": "string",
           "Endpoints": {
                  "string": "string"
           }
    },
    "DomainEndpointOptions": {
           "EnforceHTTPS": boolean,
           "TLSSecurityPolicy": "string"
    },
    "ElasticsearchClusterConfig": {
           "DedicatedMasterCount": number,
           "DedicatedMasterEnabled": boolean,
           "DedicatedMasterType": "string",
           "InstanceCount": number,
           "InstanceType": "string",
           "ZoneAwarenessConfig": {
                  "AvailabilityZoneCount": number
           },
           "ZoneAwarenessEnabled": boolean
    },
    "ElasticsearchVersion": "string",
    "EncryptionAtRestOptions": {
           "Enabled": boolean,
           "KmsKeyId": "string"
    },
    "LogPublishingOptions": {
           "AuditLogs": {
```

```
                "CloudWatchLogsLogGroupArn": "string",
                "Enabled": boolean
            },
            "IndexSlowLogs": {
                "CloudWatchLogsLogGroupArn": "string",
                "Enabled": boolean
            },
            "SearchSlowLogs": {
                "CloudWatchLogsLogGroupArn": "string",
                "Enabled": boolean
            }
    },
    "NodeToNodeEncryptionOptions": {
            "Enabled": boolean
    },
    "ServiceSoftwareOptions": {
            "AutomatedUpdateDate": "string",
            "Cancellable": boolean,
            "CurrentVersion": "string",
            "Description": "string",
            "NewVersion": "string",
            "UpdateAvailable": boolean,
            "UpdateStatus": "string"
    },
    "VPCOptions": {
            "AvailabilityZones": [
                "string"
            ],
            "SecurityGroupIds": [
                "string"
            ],
            "SubnetIds": [
                "string"
            ],
           "VPCId": "string"
    }
}
```

AwsElb

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsElb` recursos.

AwsElbLoadBalancer

O objeto `AwsElbLoadBalancer` contém detalhes sobre um Classic Load Balancer.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsElbLoadBalancer` objeto. Para ver as descrições dos `AwsElbLoadBalancer` atributos, consulte AwsElbLoadBalancerDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsElbLoadBalancer": {
    "AvailabilityZones": ["us-west-2a"],
    "BackendServerDescriptions": [
         {
            "InstancePort": 80,
            "PolicyNames": ["doc-example-policy"]
        }
    ],
    "CanonicalHostedZoneName": "Z3DZXE0EXAMPLE",
    "CanonicalHostedZoneNameID": "my-load-balancer-444455556666.us-
west-2.elb.amazonaws.com",
    "CreatedTime": "2020-08-03T19:22:44.637Z",
    "DnsName": "my-load-balancer-444455556666.us-west-2.elb.amazonaws.com",
    "HealthCheck": {
        "HealthyThreshold": 2,
        "Interval": 30,
        "Target": "HTTP:80/png",
        "Timeout": 3,
        "UnhealthyThreshold": 2
    },
    "Instances": [
        {
            "InstanceId": "i-example"
        }
    ],
    "ListenerDescriptions": [
        {
            "Listener": {
                "InstancePort": 443,
                "InstanceProtocol": "HTTPS",
                "LoadBalancerPort": 443,
                "Protocol": "HTTPS",
                "SslCertificateId": "arn:aws:iam::444455556666:server-certificate/my-
server-cert"
```

```
            },
            "PolicyNames": ["ELBSecurityPolicy-TLS-1-2-2017-01"]
        }
    ],
    "LoadBalancerAttributes": {
        "AccessLog": {
            "EmitInterval": 60,
            "Enabled": true,
            "S3BucketName": "doc-example-bucket",
            "S3BucketPrefix": "doc-example-prefix"
        },
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        },
        "ConnectionSettings": {
            "IdleTimeout": 30
        },
        "CrossZoneLoadBalancing": {
            "Enabled": true
        },
        "AdditionalAttributes": [{
            "Key": "elb.http.desyncmitigationmode",
            "Value": "strictest"
        }]

    },
    "LoadBalancerName": "example-load-balancer",
    "Policies": {
        "AppCookieStickinessPolicies": [
            {
                "CookieName": "",
                "PolicyName": ""
            }
        ],
        "LbCookieStickinessPolicies": [
            {
                "CookieExpirationPeriod": 60,
                "PolicyName": "my-example-cookie-policy"
            }
        ],
        "OtherPolicies": [
            "my-PublicKey-policy",
            "my-authentication-policy",
```

```
            "my-SSLNegotiation-policy",
            "my-ProxyProtocol-policy",
            "ELBSecurityPolicy-2015-03"
        ]
    },
    "Scheme": "internet-facing",
    "SecurityGroups": ["sg-example"],
    "SourceSecurityGroup": {
        "GroupName": "my-elb-example-group",
        "OwnerAlias": "444455556666"
    },
    "Subnets": ["subnet-example"],
    "VpcId": "vpc-a01106c2"
}
```

AwsElbv2LoadBalancer

O objeto `AwsElbv2LoadBalancer` fornece informações sobre um load balancer.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsElbv2LoadBalancer` objeto. Para ver as descrições dos `AwsElbv2LoadBalancer` atributos, consulte AwsElbv2 LoadBalancerDetails na Referência AWS Security Hub da API.

Exemplo

```
"AwsElbv2LoadBalancer": {
                        "AvailabilityZones": {
                            "SubnetId": "string",
                            "ZoneName": "string"
                        },
                        "CanonicalHostedZoneId": "string",
                        "CreatedTime": "string",
                        "DNSName": "string",
                        "IpAddressType": "string",
                        "LoadBalancerAttributes": [
                            {
                                "Key": "string",
                                "Value": "string"
                            }
                        ],
                        "Scheme": "string",
                        "SecurityGroups": [ "string" ],
                        "State": {
```

```
                        "Code": "string",
                        "Reason": "string"
                    },
                    "Type": "string",
                    "VpcId": "string"
                }
```

AwsEventBridge

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsEventBridge` recursos.

AwsEventSchemasRegistry

O `AwsEventSchemasRegistry` objeto fornece informações sobre um registro do EventBridge esquema da Amazon. Um esquema define a estrutura dos eventos para os quais são enviados EventBridge. Os registros coletam e organizam esquemas para que os esquemas estejam em grupos lógicos.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEventSchemasRegistry` objeto. Para ver as descrições dos `AwsEventSchemasRegistry` atributos, consulte AwsEventSchemasRegistryna Referência AWS Security Hub da API.

Exemplo

```
"AwsEventSchemasRegistry": {
    "Description": "This is an example event schema registry.",
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
    "RegistryName": "schema-registry"
}
```

AwsEventsEndpoint

O `AwsEventsEndpoint` objeto fornece informações sobre um endpoint EventBridge global da Amazon. Um endpoint global usado para melhorar a disponibilidade da sua aplicação, tornando-a tolerante a falhas regionais.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEventsEndpoint` objeto. Para ver as descrições dos `AwsEventsEndpoint` atributos, consulte AwsEventsEndpointDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsEventsEndpoint": {
    "Arn": "arn:aws:events:us-east-1:123456789012:endpoint/my-endpoint",
    "Description": "This is a sample endpoint.",
    "EndpointId": "04k1exajoy.veo",
    "EndpointUrl": "https://04k1exajoy.veo.endpoint.events.amazonaws.com",
    "EventBuses": [
        {
            "EventBusArn": "arn:aws:events:us-east-1:123456789012:event-bus/default"
        },
        {
            "EventBusArn": "arn:aws:events:us-east-2:123456789012:event-bus/default"
        }
    ],
    "Name": "my-endpoint",
    "ReplicationConfig": {
        "State": "ENABLED"
    },
    "RoleArn": "arn:aws:iam::123456789012:role/service-role/
Amazon_EventBridge_Invoke_Event_Bus_1258925394",
    "RoutingConfig": {
        "FailoverConfig": {
            "Primary": {
                "HealthCheck": "arn:aws:route53:::healthcheck/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
            },
            "Secondary": {
                "Route": "us-east-2"
            }
        }
    },
    "State": "ACTIVE"
}
```

AwsEventsEventbus

O `AwsEventsEventbus` objeto fornece informações sobre um endpoint EventBridge global da Amazon. Um endpoint global usado para melhorar a disponibilidade da sua aplicação, tornando-a tolerante a falhas regionais.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsEventsEventbus` objeto. Para ver as descrições dos `AwsEventsEventbus` atributos, consulte AwsEventsEventbusDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsEventsEventbus":
    "Arn": "arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus",
    "Name": "my-event-bus",
    "Policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AllowAllAccountsFromOrganizationToPutEvents\",\"Effect\":\"Allow
\",\"Principal\":\"*\",\"Action\":\"events:PutEvents\",\"Resource\":
\"arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus\",\"Condition
\":{\"StringEquals\":{\"aws:PrincipalOrgID\":\"o-ki7yjtkjv5\"}}},{\"Sid\":
\"AllowAccountToManageRulesTheyCreated\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
\"arn:aws:iam::123456789012:root\"},\"Action\":[\"events:PutRule\",\"events:PutTargets
\",\"events:DeleteRule\",\"events:RemoveTargets\",\"events:DisableRule
\",\"events:EnableRule\",\"events:TagResource\",\"events:UntagResource\",
\"events:DescribeRule\",\"events:ListTargetsByRule\",\"events:ListTagsForResource\"],
\"Resource\":\"arn:aws:events:us-east-1:123456789012:rule/my-event-bus\",\"Condition\":
{\"StringEqualsIfExists\":{\"events:creatorAccount\":\"123456789012\"}}}]}"
```

AwsGuardDuty

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsGuardDuty` recursos.

AwsGuardDutyDetector

O `AwsGuardDutyDetector` objeto fornece informações sobre um GuardDuty detector da Amazon. Um detector é um objeto que representa o GuardDuty serviço. É necessário um detector GuardDuty para se tornar operacional.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsGuardDutyDetector` objeto. Para ver as descrições dos `AwsGuardDutyDetector` atributos, consulte AwsGuardDutyDetectorna Referência AWS Security Hub da API.

Exemplo

```
"AwsGuardDutyDetector": {
    "FindingPublishingFrequency": "SIX_HOURS",
    "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Status": "ENABLED",
    "DataSources": {
        "CloudTrail": {
            "Status": "ENABLED"
```

```
        },
        "DnsLogs": {
            "Status": "ENABLED"
        },
        "FlowLogs": {
            "Status": "ENABLED"
        },
        "S3Logs": {
             "Status": "ENABLED"
         },
         "Kubernetes": {
             "AuditLogs": {
                "Status": "ENABLED"
             }
         },
         "MalwareProtection": {
             "ScanEc2InstanceWithFindings": {
                "EbsVolumes": {
                    "Status": "ENABLED"
                 }
             },
            "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/malware-
protection.guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDutyMalwareProtection"
         }
    }
}
```

AwsIam

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsIam` recursos.

AwsIamAccessKey

O objeto `AwsIamAccessKey` contém detalhes sobre uma chave de acesso do IAM relacionada a uma descoberta.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsIamAccessKey` objeto. Para ver as descrições dos `AwsIamAccessKey` atributos, consulte AwsIamAccessKeyDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsIamAccessKey": {
                        "AccessKeyId": "string",
```

```
                        "AccountId": "string",
                        "CreatedAt": "string",
                        "PrincipalId": "string",
                        "PrincipalName": "string",
                        "PrincipalType": "string",
                        "SessionContext": {
                            "Attributes": {
                                "CreationDate": "string",
                                "MfaAuthenticated": boolean
                            },
                            "SessionIssuer": {
                                "AccountId": "string",
                                "Arn": "string",
                                "PrincipalId": "string",
                                "Type": "string",
                                "UserName": "string"
                            }
                        },
                        "Status": "string"
                    }
```

AwsIamGroup

O objeto `AwsIamGroup` contém detalhes sobre um grupo IAM.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsIamGroup` objeto. Para ver as descrições dos `AwsIamGroup` atributos, consulte AwsIamGroupDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsIamGroup": {
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleManagedAccess",
            "PolicyName": "ExampleManagedAccess",
        }
    ],
    "CreateDate": "2020-04-28T14:08:37.000Z",
    "GroupId": "AGPA4TPS3VLP7QEXAMPLE",
    "GroupName": "Example_User_Group",
    "GroupPolicyList": [
        {
```

```
            "PolicyName": "ExampleGroupPolicy"
        }
    ],
    "Path": "/"
}
```

AwsIamPolicy

O objeto `AwsIamPolicy` representa uma política de permissões do IAM.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsIamPolicy` objeto. Para ver as descrições dos `AwsIamPolicy` atributos, consulte AwsIamPolicyDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsIamPolicy": {
    "AttachmentCount": 1,
    "CreateDate": "2017-09-14T08:17:29.000Z",
    "DefaultVersionId": "v1",
    "Description": "Example IAM policy",
    "IsAttachable": true,
    "Path": "/",
    "PermissionsBoundaryUsageCount": 5,
    "PolicyId": "ANPAJ2UCCR6DPCEXAMPLE",
    "PolicyName": "EXAMPLE-MANAGED-POLICY",
    "PolicyVersionList": [
        {
            "VersionId": "v1",
            "IsDefaultVersion": true,
            "CreateDate": "2017-09-14T08:17:29.000Z"
        }
    ],
    "UpdateDate": "2017-09-14T08:17:29.000Z"
}
```

AwsIamRole

Contém informações sobre uma função do IAM, incluindo todas as políticas da função.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsIamRole` objeto. Para ver as descrições dos `AwsIamRole` atributos, consulte AwsIamRoleDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsIamRole": {
    "AssumeRolePolicyDocument": "{'Version': '2012-10-17','Statement': [{'Effect':
 'Allow','Action': 'sts:AssumeRole'}]}",
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExamplePolicy1",
            "PolicyName": "Example policy 1"
        },
        {
            "PolicyArn": "arn:aws:iam::444455556666:policy/ExamplePolicy2",
            "PolicyName": "Example policy 2"
        }
        ],
        "CreateDate": "2020-03-14T07:19:14.000Z",
        "InstanceProfileList": [
            {
                "Arn": "arn:aws:iam::333333333333:ExampleProfile",
                "CreateDate": "2020-03-11T00:02:27Z",
                "InstanceProfileId": "AIPAIXEU4NUHUPEXAMPLE",
                "InstanceProfileName": "ExampleInstanceProfile",
                "Path": "/",
                "Roles": [
                    {
                       "Arn": "arn:aws:iam::444455556666:role/example-role",
                        "AssumeRolePolicyDocument": "",
                        "CreateDate": "2020-03-11T00:02:27Z",
                        "Path": "/",
                        "RoleId": "AROAJ52OTH4H7LEXAMPLE",
                        "RoleName": "example-role",
                    }
                ]
            }
        ],
        "MaxSessionDuration": 3600,
        "Path": "/",
        "PermissionsBoundary": {
            "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
            "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
        },
        "RoleId": "AROA4TPS3VLEXAMPLE",
        "RoleName": "BONESBootstrapHydra-OverbridgeOpsFunctionsLambda",
        "RolePolicyList": [
```

```
            {
                "PolicyName": "Example role policy"
            }
        ]
    }
```

AwsIamUser

O objeto `AwsIamUser` fornece informações sobre um usuário.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsIamUser` objeto. Para ver as descrições dos `AwsIamUser` atributos, consulte AwsIamUserDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsIamUser": {
    "AttachedManagedPolicies": [
        {
            "PolicyName": "ExamplePolicy",
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleAccess"
        }
    ],
    "CreateDate": "2018-01-26T23:50:05.000Z",
    "GroupList": [],
    "Path": "/",
    "PermissionsBoundary" : {
        "PermissionsBoundaryArn" : "arn:aws:iam::aws:policy/AdministratorAccess",
        "PermissionsBoundaryType" : "PermissionsBoundaryPolicy"
    },
    "UserId": "AIDACKCEVSQ6C2EXAMPLE",
    "UserName": "ExampleUser",
    "UserPolicyList": [
        {
            "PolicyName": "InstancePolicy"
        }
    ]
}
```

AwsKinesis

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsKinesis` recursos.

AwsKinesisStream

O objeto `AwsKinesisStream` fornece detalhes sobre o Amazon Kinesis Data Streams.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsKinesisStream` objeto. Para ver as descrições dos `AwsKinesisStream` atributos, consulte AwsKinesisStreamDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsKinesisStream": {
 "Name": "test-vir-kinesis-stream",
 "Arn": "arn:aws:kinesis:us-east-1:293279581038:stream/test-vir-kinesis-stream",
 "RetentionPeriodHours": 24,
 "ShardCount": 2,
 "StreamEncryption": {
  "EncryptionType": "KMS",
  "KeyId": "arn:aws:kms:us-east-1:293279581038:key/849cf029-4143-4c59-91f8-
ea76007247eb"
 }
}
```

AwsKms

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsKms` recursos.

AwsKmsKey

O `AwsKmsKey` objeto fornece detalhes sobre um AWS KMS key.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsKmsKey` objeto. Para ver as descrições dos `AwsKmsKey` atributos, consulte AwsKmsKeyDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsKmsKey": {
                        "AWSAccountId": "string",
                        "CreationDate": "string",
                        "Description": "string",
                        "KeyId": "string",
```

```
                    "KeyManager": "string",
                    "KeyRotationStatus": boolean,
                    "KeyState": "string",
                    "Origin": "string"
                }
```

AwsLambda

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsLambda` recursos.

AwsLambdaFunction

O objeto fornece detalhes sobre a configuração de uma função do .

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsLambdaFunction` objeto. Para ver as descrições dos `AwsLambdaFunction` atributos, consulte AwsLambdaFunctionDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsLambdaFunction": {
    "Architectures": [
        "x86_64"
    ],
    "Code": {
        "S3Bucket": "DOC-EXAMPLE-BUCKET",
        "S3Key": "samplekey",
        "S3ObjectVersion": "2",
        "ZipFile": "myzip.zip"
    },
    "CodeSha256": "1111111111111abcdef",
    "DeadLetterConfig": {
        "TargetArn": "arn:aws:lambda:us-east-2:123456789012:queue:myqueue:2"
    },
    "Environment": {
        "Variables": {
            "Stage": "foobar"
         },
        "Error": {
            "ErrorCode": "Sample-error-code",
            "Message": "Caller principal is a manager."
         }
     },
```

```
    "FunctionName": "CheckOut",
    "Handler": "main.py:lambda_handler",
    "KmsKeyArn": "arn:aws:kms:us-west-2:123456789012:key/mykey",
    "LastModified": "2001-09-11T09:00:00Z",
    "Layers": {
        "Arn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:3",
        "CodeSize": 169
    },
    "PackageType": "Zip",
    "RevisionId": "23",
    "Role": "arn:aws:iam::123456789012:role/Accounting-Role",
    "Runtime": "go1.7",
    "Timeout": 15,
    "TracingConfig": {
        "Mode": "Active"
    },
    "Version": "$LATEST$",
    "VpcConfig": {
        "SecurityGroupIds": ["sg-085912345678492fb", "sg-08591234567bdgdc"],
         "SubnetIds": ["subnet-071f712345678e7c8", "subnet-07fd123456788a036"]
    },
    "MasterArn": "arn:aws:lambda:us-east-2:123456789012:\$LATEST",
    "MemorySize": 2048
}
```

AwsLambdaLayerVersion

O objeto fornece detalhes sobre uma versão da camada do .

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsLambdaLayerVersion` objeto. Para ver as descrições dos `AwsLambdaLayerVersion` atributos, consulte AwsLambdaLayerVersionDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsLambdaLayerVersion": {
    "Version": 2,
    "CompatibleRuntimes": [
        "java8"
    ],
    "CreatedDate": "2019-10-09T22:02:00.274+0000"
}
```

AwsMsk

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsMsk` recursos.

AwsMskCluster

O objeto `AwsMskCluster` fornece informações sobre um cluster do Amazon Managed Streaming for Apache Kafka (Amazon MSK).

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsMskCluster` objeto. Para ver as descrições dos `AwsMskCluster` atributos, consulte AwsMskClusterDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsMskCluster": {
        "ClusterInfo": {
            "ClientAuthentication": {
                "Sasl": {
                    "Scram": {
                        "Enabled": true
                    },
                    "Iam": {
                        "Enabled": true
                    }
                },
                "Tls": {
                    "CertificateAuthorityArnList": [],
                    "Enabled": false
                },
                "Unauthenticated": {
                    "Enabled": false
                }
            },
            "ClusterName": "my-cluster",
            "CurrentVersion": "K2PWKAKR8XB7XF",
            "EncryptionInfo": {
                "EncryptionAtRest": {
                    "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
                },
                "EncryptionInTransit": {
                    "ClientBroker": "TLS",
```

```
                    "InCluster": true
                }
            },
            "EnhancedMonitoring": "PER_TOPIC_PER_BROKER",
            "NumberOfBrokerNodes": 3
        }
}
```

AwsNetworkFirewall

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsNetworkFirewall` recursos.

AwsNetworkFirewallFirewall

O objeto contém detalhes sobre um trabalho.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsNetworkFirewallFirewall` objeto. Para ver as descrições dos `AwsNetworkFirewallFirewall` atributos, consulte AwsNetworkFirewallFirewallDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsNetworkFirewallFirewall": {
    "DeleteProtection": false,
    "FirewallArn": "arn:aws:network-firewall:us-east-1:024665936331:firewall/
testfirewall",
    "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
    "FirewallId": "dea7d8e9-ae38-4a8a-b022-672a830a99fa",
    "FirewallName": "testfirewall",
    "FirewallPolicyChangeProtection": false,
    "SubnetChangeProtection": false,
    "SubnetMappings": [
        {
            "SubnetId": "subnet-0183481095e588cdc"
        },
        {
            "SubnetId": "subnet-01f518fad1b1c90b0"
        }
    ],
    "VpcId": "vpc-40e83c38"
```

```
}
```

AwsNetworkFirewallFirewallPolicy

O objeto `AwsNetworkFirewallFirewallPolicy` fornece detalhes sobre uma política de firewall. Uma política de firewall define o comportamento de um firewall de rede.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsNetworkFirewallFirewallPolicy` objeto. Para ver as descrições dos `AwsNetworkFirewallFirewallPolicy` atributos, consulte AwsNetworkFirewallFirewallPolicyDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsNetworkFirewallFirewallPolicy": {
   "FirewallPolicy": {
    "StatefulRuleGroupReferences": [
        {
            "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/PatchesOnly"
        }
    ],
    "StatelessDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessRuleGroupReferences": [
       {
          "Priority": 1,
          "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1"
       }
     ]
   },
   "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
   "FirewallPolicyId": "9ceeda22-6050-4048-a0ca-50ce47f0cc65",
   "FirewallPolicyName": "InitialFirewall",
   "Description": "Initial firewall"
}
```

AwsNetworkFirewallRuleGroup

O objeto `AwsNetworkFirewallRuleGroup` fornece detalhes sobre uma WebACL do AWS Network Firewall . O usa um grupo de regras para inspecionar e controlar o tráfego de rede. Os

grupos de regras sem estado se aplicam a pacotes individuais. É possível igualmente definir grupos de regras com estado para inspecionar pacotes no contexto do fluxo de tráfego.

Os grupos de regras são referenciados nas políticas de firewall.

Os exemplos a seguir mostram o AWS Security Finding Format (ASFF) do `AwsNetworkFirewallRuleGroup` objeto. Para ver as descrições dos `AwsNetworkFirewallRuleGroup` atributos, consulte AwsNetworkFirewallRuleGroupDetailsna Referência AWS Security Hub da API.

Exemplo — grupo de regras sem estado

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 600,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1",
    "RuleGroupId": "fb13c4df-b6da-4c1e-91ec-84b7a5487493",
    "RuleGroupName": "Stateless-1"
    "Description": "Example of a stateless rule group",
    "Type": "STATELESS",
    "RuleGroup": {
        "RulesSource": {
            "StatelessRulesAndCustomActions": {
                "CustomActions": [],
                "StatelessRules": [
                    {
                        "Priority": 1,
                        "RuleDefinition": {
                            "Actions": [
                                "aws:pass"
                            ],
                            "MatchAttributes": {
                                "DestinationPorts": [
                                    {
                                        "FromPort": 443,
                                        "ToPort": 443
                                    }
                                ],
                                "Destinations": [
                                    {
                                        "AddressDefinition": "192.0.2.0/24"
                                    }
                                ],
```

```
                                "Protocols": [
                                            6
                                ],
                                "SourcePorts": [
                                    {
                                        "FromPort": 0,
                                        "ToPort": 65535
                                    }
                                ],
                                "Sources": [
                                    {
                                         "AddressDefinition": "198.51.100.0/24"
                                    }
                                ]
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

Exemplo — grupo de regras com estado

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 100,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/tupletest",
    "RuleGroupId": "38b71c12-da80-4643-a6c5-03337f8933e0",
    "RuleGroupName": "ExampleRuleGroup",
    "Description": "Example of a stateful rule group",
    "Type": "STATEFUL",
    "RuleGroup": {
        "RuleSource": {
             "StatefulRules": [
                 {
                     "Action": "PASS",
                     "Header": {
                         "Destination": "Any",
                         "DestinationPort": "443",
                         "Direction": "ANY",
                         "Protocol": "TCP",
```

```
                        "Source": "Any",
                        "SourcePort": "Any"
                    },
                    "RuleOptions": [
                        {
                           "Keyword": "sid:1"
                        }
                    ]
                }
            ]
        }
    }
}
```

Veja a seguir uma lista de exemplos de valores válidos para atributos `AwsNetworkFirewallRuleGroup`:

- `Action`

  Valores válidos: `PASS` | `DROP` | `ALERT`

- `Protocol`

  Valores válidos`TCP`: `UDP` | `ICMP` | `HTTP` | `FTP` | `TLS` | `SMB` | `DNS` | `DCERPC` | `SSH` | `SMTP` | `IMAP` | `MSN` | `KRB5` | `IKEV2` | `TFTP` | `NTP` | | | |

- `Flags`

  Valores válidos: `FIN` | `SYN` | `RST` | `PSH` | `ACK` | `URG` | `ECE` | `CWR`

- `Masks`

  Valores válidos: `FIN` | `SYN` | `RST` | `PSH` | `ACK` | `URG` | `ECE` | `CWR`

AwsOpenSearchService

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsOpenSearchService` recursos.

AwsOpenSearchServiceDomain

O `AwsOpenSearchServiceDomain` objeto contém informações sobre um domínio do Amazon OpenSearch Service.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsOpenSearchServiceDomain` objeto. Para ver as descrições dos `AwsOpenSearchServiceDomain` atributos, consulte AwsOpenSearchServiceDomainDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsOpenSearchServiceDomain": {
    "AccessPolicies": "IAM_Id",
    "AdvancedSecurityOptions": {
        "Enabled": true,
        "InternalUserDatabaseEnabled": true,
        "MasterUserOptions": {
            "MasterUserArn": "arn:aws:iam::123456789012:user/third-master-use",
            "MasterUserName": "third-master-use",
            "MasterUserPassword": "some-password"
        }
    },
    "Arn": "arn:aws:Opensearch:us-east-1:111122223333:somedomain",
    "ClusterConfig": {
        "InstanceType": "c5.large.search",
        "InstanceCount": 1,
        "DedicatedMasterEnabled": true,
        "ZoneAwarenessEnabled": false,
        "ZoneAwarenessConfig": {
            "AvailabilityZoneCount": 2
        },
        "DedicatedMasterType": "c5.large.search",
        "DedicatedMasterCount": 3,
        "WarmEnabled": true,
        "WarmCount": 3,
        "WarmType": "ultrawarm1.large.search"
    },
    "DomainEndpoint": "https://es-2021-06-23t17-04-qowmgghud5vofgb5e4wmi.eu-
central-1.es.amazonaws.com",
    "DomainEndpointOptions": {
        "EnforceHTTPS": false,
        "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07",
        "CustomEndpointCertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/bda1bff1-79c0-49d0-abe6-50a15a7477d4",
        "CustomEndpointEnabled": true,
        "CustomEndpoint": "example.com"
    },
```

```
    "DomainEndpoints": {
        "vpc": "vpc-endpoint-h2dsd34efgyghrtguk5gt6j2foh4.us-east-1.es.amazonaws.com"
    },
    "DomainName": "my-domain",
    "EncryptionAtRestOptions": {
        "Enabled": false,
        "KmsKeyId": "1a2a3a4-1a2a-3a4a-5a6a-1a2a3a4a5a6a"
    },
    "EngineVersion": "7.1",
    "Id": "123456789012",
    "LogPublishingOptions": {
        "IndexSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-index-slow-logs",
            "Enabled": true
        },
        "SearchSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        },
        "AuditLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        }
    },
    "NodeToNodeEncryptionOptions": {
        "Enabled": true
    },
    "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "2022-04-28T14:08:37.000Z",
        "Cancellable": false,
        "CurrentVersion": "R20210331",
        "Description": "There is no software update available for this domain.",
        "NewVersion": "OpenSearch_1.0",
        "UpdateAvailable": false,
        "UpdateStatus": "COMPLETED",
        "OptionalDeployment": false
    },
    "VpcOptions": {
        "SecurityGroupIds": [
            "sg-2a3a4a5a"
        ],
```

```
        "SubnetIds": [
            "subnet-1a2a3a4a"
        ],
    }
}
```

AwsRds

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsRds` recursos.

AwsRdsDbCluster

O objeto `AwsRdsDbCluster` fornece detalhes sobre um cluster de banco de dados do Amazon RDS.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsRdsDbCluster` objeto. Para ver as descrições dos `AwsRdsDbCluster` atributos, consulte AwsRdsDbClusterDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsRdsDbCluster": {
    "ActivityStreamStatus": "stopped",
    "AllocatedStorage": 1,
    "AssociatedRoles": [
        {
        "RoleArn": "arn:aws:iam::777788889999:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
        "Status": "PENDING"
        }
    ],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1c",
        "us-east-1e"
    ],
    "BackupRetentionPeriod": 1,
    "ClusterCreateTime": "2020-06-22T17:40:12.322Z",
    "CopyTagsToSnapshot": true,
    "CrossAccountClone": false,
    "CustomEndpoints": [],
    "DatabaseName": "Sample name",
    "DbClusterIdentifier": "database-3",
```

```
    "DbClusterMembers": [
        {
        "DbClusterParameterGroupStatus": "in-sync",
        "DbInstanceIdentifier": "database-3-instance-1",
        "IsClusterWriter": true,
        "PromotionTier": 1,
        }
    ],
    "DbClusterOptionGroupMemberships": [],
    "DbClusterParameterGroup": "cluster-parameter-group",
    "DbClusterResourceId": "cluster-example",
    "DbSubnetGroup": "subnet-group",
    "DeletionProtection": false,
    "DomainMemberships": [],
    "Status": "modifying",
    "EnabledCloudwatchLogsExports": [
        "audit",
        "error",
        "general",
        "slowquery"
    ],
    "Endpoint": "database-3.cluster-example.us-east-1.rds.amazonaws.com",
    "Engine": "aurora-mysql",
    "EngineMode": "provisioned",
    "EngineVersion": "5.7.mysql_aurora.2.03.4",
    "HostedZoneId": "ZONE1",
    "HttpEndpointEnabled": false,
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "MasterUsername": "admin",
    "MultiAz": false,
    "Port": 3306,
    "PreferredBackupWindow": "04:52-05:22",
    "PreferredMaintenanceWindow": "sun:09:32-sun:10:02",
    "ReaderEndpoint": "database-3.cluster-ro-example.us-east-1.rds.amazonaws.com",
    "ReadReplicaIdentifiers": [],
    "Status": "Modifying",
    "StorageEncrypted": true,
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example-1"
        }
    ],
```

```
}
```

AwsRdsDbClusterSnapshot

O objeto `AwsRdsDbClusterSnapshot` contém informações sobre um instantâneo de cluster de banco de dados do Amazon RDS.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsRdsDbClusterSnapshot` objeto. Para ver as descrições dos `AwsRdsDbClusterSnapshot` atributos, consulte AwsRdsDbClusterSnapshotDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsRdsDbClusterSnaphot": {
    "AllocatedStorage": 0,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1d",
        "us-east-1e"
    ],
    "ClusterCreateTime": "2020-06-12T13:23:15.577Z",
    "DbClusterIdentifier": "database-2",
    "DbClusterSnapshotAttributes": [{
        "AttributeName": "restore",
        "AttributeValues": ["123456789012"]
    }],
    "DbClusterSnapshotIdentifier": "rds:database-2-2020-06-23-03-52",
    "Engine": "aurora",
    "EngineVersion": "5.6.10a",
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "LicenseModel": "aurora",
    "MasterUsername": "admin",
    "PercentProgress": 100,
    "Port": 0,
    "SnapshotCreateTime": "2020-06-22T17:40:12.322Z",
    "SnapshotType": "automated",
    "Status": "available",
    "StorageEncrypted": true,
    "VpcId": "vpc-faf7e380"
}
```

AwsRdsDbInstance

O objeto fornece detalhes sobre uma instância de banco de dados do Amazon RDS.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsRdsDbInstance` objeto. Para ver as descrições dos `AwsRdsDbInstance` atributos, consulte AwsRdsDbInstanceDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsRdsDbInstance": {
    "AllocatedStorage": 20,
    "AssociatedRoles": [],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1d",
    "BackupRetentionPeriod": 7,
    "CaCertificateIdentifier": "certificate1",
    "CharacterSetName": "",
    "CopyTagsToSnapshot": true,
    "DbClusterIdentifier": "",
    "DbInstanceArn": "arn:aws:rds:us-east-1:111122223333:db:database-1",
    "DbInstanceClass": "db.t2.micro",
    "DbInstanceIdentifier": "database-1",
    "DbInstancePort": 0,
    "DbInstanceStatus": "available",
    "DbiResourceId": "db-EXAMPLE123",
    "DbName": "",
    "DbParameterGroups": [
        {
            "DbParameterGroupName": "default.mysql5.7",
            "ParameterApplyStatus": "in-sync"
        }
    ],
    "DbSecurityGroups": [],


    "DbSubnetGroup": {
        "DbSubnetGroupName": "my-group-123abc",
        "DbSubnetGroupDescription": "My subnet group",
        "VpcId": "vpc-example1",
        "SubnetGroupStatus": "Complete",
        "Subnets": [
            {
                "SubnetIdentifier": "subnet-123abc",
```

```
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1d"
                },
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-456def",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1c"
                },
                "SubnetStatus": "Active"
            }
      ],
        "DbSubnetGroupArn": ""
    },
    "DeletionProtection": false,
    "DomainMemberships": [],
    "EnabledCloudWatchLogsExports": [],
    "Endpoint": {
        "address": "database-1.example.us-east-1.rds.amazonaws.com",
        "port": 3306,
        "hostedZoneId": "ZONEID1"
    },
    "Engine": "mysql",
    "EngineVersion": "5.7.22",
    "EnhancedMonitoringResourceArn": "arn:aws:logs:us-east-1:111122223333:log-
group:Example:log-stream:db-EXAMPLE1",
    "IamDatabaseAuthenticationEnabled": false,
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "Iops": "",
    "KmsKeyId": "",
    "LatestRestorableTime": "2020-06-24T05:50:00.000Z",
    "LicenseModel": "general-public-license",
    "ListenerEndpoint": "",
    "MasterUsername": "admin",
    "MaxAllocatedStorage": 1000,
    "MonitoringInterval": 60,
    "MonitoringRoleArn": "arn:aws:iam::111122223333:role/rds-monitoring-role",
    "MultiAz": false,
    "OptionGroupMemberships": [
        {
            "OptionGroupName": "default:mysql-5-7",
            "Status": "in-sync"
        }
```

```
    ],
    "PreferredBackupWindow": "03:57-04:27",
    "PreferredMaintenanceWindow": "thu:10:13-thu:10:43",
    "PendingModifiedValues": {
        "DbInstanceClass": "",
        "AllocatedStorage": "",
        "MasterUserPassword": "",
        "Port": "",
        "BackupRetentionPeriod": "",
        "MultiAZ": "",
        "EngineVersion": "",
        "LicenseModel": "",
        "Iops": "",
        "DbInstanceIdentifier": "",
        "StorageType": "",
        "CaCertificateIdentifier": "",
        "DbSubnetGroupName": "",
        "PendingCloudWatchLogsExports": "",
        "ProcessorFeatures": []
    },
    "PerformanceInsightsEnabled": false,
    "PerformanceInsightsKmsKeyId": "",
    "PerformanceInsightsRetentionPeriod": "",
    "ProcessorFeatures": [],
    "PromotionTier": "",
    "PubliclyAccessible": false,
    "ReadReplicaDBClusterIdentifiers": [],
    "ReadReplicaDBInstanceIdentifiers": [],
    "ReadReplicaSourceDBInstanceIdentifier": "",
    "SecondaryAvailabilityZone": "",
    "StatusInfos": [],
    "StorageEncrypted": false,
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Timezone": "",
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-example1",
            "Status": "active"
        }
    ]
}
```

AwsRdsDbSecurityGroup

Um objeto contendo informações sobre a configuração do Amazon Relational Database Service (RDS).

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsRdsDbSecurityGroup` objeto. Para ver as descrições dos `AwsRdsDbSecurityGroup` atributos, consulte AwsRdsDbSecurityGroupDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsRdsDbSecurityGroup": {
    "DbSecurityGroupArn": "arn:aws:rds:us-west-1:111122223333:secgrp:default",
    "DbSecurityGroupDescription": "default",
    "DbSecurityGroupName": "mysecgroup",
    "Ec2SecurityGroups": [
        {
          "Ec2SecurityGroupuId": "myec2group",
          "Ec2SecurityGroupName": "default",
          "Ec2SecurityGroupOwnerId": "987654321021",
          "Status": "authorizing"
        }
    ],
    "IpRanges": [
        {
          "Cidrip": "0.0.0.0/0",
          "Status": "authorizing"
        }
    ],
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234567f"
}
```

AwsRdsDbSnapshot

O objeto `AwsRdsDbSnapshot` contém informações sobre um instantâneo de cluster de banco de dados do Amazon RDS.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsRdsDbSnapshot` objeto. Para ver as descrições dos `AwsRdsDbSnapshot` atributos, consulte AwsRdsDbSnapshotDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsRdsDbSnapshot": {
    "DbSnapshotIdentifier": "rds:database-1-2020-06-22-17-41",
    "DbInstanceIdentifier": "database-1",
    "SnapshotCreateTime": "2020-06-22T17:41:29.967Z",
    "Engine": "mysql",
    "AllocatedStorage": 20,
    "Status": "available",
    "Port": 3306,
    "AvailabilityZone": "us-east-1d",
    "VpcId": "vpc-example1",
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "MasterUsername": "admin",
    "EngineVersion": "5.7.22",
    "LicenseModel": "general-public-license",
    "SnapshotType": "automated",
    "Iops": null,
    "OptionGroupName": "default:mysql-5-7",
    "PercentProgress": 100,
    "SourceRegion": null,
    "SourceDbSnapshotIdentifier": "",
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Encrypted": false,
    "KmsKeyId": "",
    "Timezone": "",
    "IamDatabaseAuthenticationEnabled": false,
    "ProcessorFeatures": [],
    "DbiResourceId": "db-resourceexample1"
}
```

AwsRdsEventSubscription

O `AwsRdsEventSubscription` contém detalhes sobre uma assinatura de notificação de evento do RDS. A assinatura permite que o RDS publique eventos em um tópico do SNS.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsRdsEventSubscription` objeto. Para ver as descrições dos `AwsRdsEventSubscription` atributos, consulte AwsRdsEventSubscriptionDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsRdsEventSubscription": {
    "CustSubscriptionId": "myawsuser-secgrp",
```

```
    "CustomerAwsId": "111111111111",
    "Enabled": true,
    "EventCategoriesList": [
        "configuration change",
        "failure"
    ],
    "EventSubscriptionArn": "arn:aws:rds:us-east-1:111111111111:es:my-instance-events",
    "SnsTopicArn": "arn:aws:sns:us-east-1:111111111111:myawsuser-RDS",
    "SourceIdsList": [
        "si-sample",
        "mysqldb-rr"
    ],
    "SourceType": "db-security-group",
    "Status": "creating",
    "SubscriptionCreationTime": "2021-06-27T01:38:01.090Z"
}
```

AwsRedshift

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsRedshift` recursos.

AwsRedshiftCluster

O objeto `AwsRedshiftCluster` contém detalhes sobre um cluster do Amazon Redshift.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsRedshiftCluster` objeto. Para ver as descrições dos `AwsRedshiftCluster` atributos, consulte AwsRedshiftClusterDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsRedshiftCluster": {
    "AllowVersionUpgrade": true,
    "AutomatedSnapshotRetentionPeriod": 1,
    "AvailabilityZone": "us-west-2d",
    "ClusterAvailabilityStatus": "Unavailable",
    "ClusterCreateTime": "2020-08-03T19:22:44.637Z",
    "ClusterIdentifier": "redshift-cluster-1",
    "ClusterNodes": [
        {
            "NodeRole": "LEADER",
            "PrivateIPAddress": "192.0.2.108",
            "PublicIPAddress": "198.51.100.29"
        },
```

```
        {
            "NodeRole": "COMPUTE-0",
            "PrivateIPAddress": "192.0.2.22",
            "PublicIPAddress": "198.51.100.63"
        },
        {
             "NodeRole": "COMPUTE-1",
             "PrivateIPAddress": "192.0.2.224",
             "PublicIPAddress": "198.51.100.226"
        }
        ],
    "ClusterParameterGroups": [
        {
            "ClusterParameterStatusList": [
                {
                    "ParameterName": "max_concurrency_scaling_clusters",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "enable_user_activity_logging",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "auto_analyze",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "query_group",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "datestyle",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "extra_float_digits",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
```

```
                {
                    "ParameterName": "search_path",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "statement_timeout",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "wlm_json_configuration",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "require_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "use_fips_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                }
            ],
            "ParameterApplyStatus": "in-sync",
            "ParameterGroupName": "temp"
        }
    ],
    "ClusterPublicKey": "JalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY Amazon-Redshift",
    "ClusterRevisionNumber": 17498,
    "ClusterSecurityGroups": [
        {
            "ClusterSecurityGroupName": "default",
            "Status": "active"
        }
    ],
    "ClusterSnapshotCopyStatus": {
        "DestinationRegion": "us-west-2",
        "ManualSnapshotRetentionPeriod": -1,
        "RetentionPeriod": 1,
        "SnapshotCopyGrantName": "snapshotCopyGrantName"
    },
```

```
    "ClusterStatus": "available",
    "ClusterSubnetGroupName": "default",
    "ClusterVersion": "1.0",
    "DBName": "dev",
    "DeferredMaintenanceWindows": [
        {
            "DeferMaintenanceEndTime": "2020-10-07T20:34:01.000Z",
            "DeferMaintenanceIdentifier": "deferMaintenanceIdentifier",
            "DeferMaintenanceStartTime": "2020-09-07T20:34:01.000Z"
        }
     ],
    "ElasticIpStatus": {
        "ElasticIp": "203.0.113.29",
        "Status": "active"
    },
    "ElasticResizeNumberOfNodeOptions": "4",
    "Encrypted": false,
    "Endpoint": {
        "Address": "redshift-cluster-1.example.us-west-2.redshift.amazonaws.com",
        "Port": 5439
    },
    "EnhancedVpcRouting": false,
    "ExpectedNextSnapshotScheduleTime": "2020-10-13T20:34:01.000Z",
    "ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
    "HsmStatus": {
        "HsmClientCertificateIdentifier": "hsmClientCertificateIdentifier",
        "HsmConfigurationIdentifier": "hsmConfigurationIdentifier",
        "Status": "applying"
    },
    "IamRoles": [
        {
             "ApplyStatus": "in-sync",
             "IamRoleArn": "arn:aws:iam::111122223333:role/RedshiftCopyUnload"
        }
    ],
    "KmsKeyId": "kmsKeyId",
    "LoggingStatus": {
        "BucketName": "test-bucket",
        "LastFailureMessage": "test message",
        "LastFailureTime": "2020-08-09T13:00:00.000Z",
        "LastSuccessfulDeliveryTime": "2020-08-08T13:00:00.000Z",
        "LoggingEnabled": true,
        "S3KeyPrefix": "/"
    },
```

```
    "MaintenanceTrackName": "current",
    "ManualSnapshotRetentionPeriod": -1,
    "MasterUsername": "awsuser",
    "NextMaintenanceWindowStartTime": "2020-08-09T13:00:00.000Z",
    "NodeType": "dc2.large",
    "NumberOfNodes": 2,
    "PendingActions": [],
    "PendingModifiedValues": {
        "AutomatedSnapshotRetentionPeriod": 0,
        "ClusterIdentifier": "clusterIdentifier",
        "ClusterType": "clusterType",
        "ClusterVersion": "clusterVersion",
        "EncryptionType": "None",
        "EnhancedVpcRouting": false,
        "MaintenanceTrackName": "maintenanceTrackName",
        "MasterUserPassword": "masterUserPassword",
        "NodeType": "dc2.large",
        "NumberOfNodes": 1,
        "PubliclyAccessible": true
    },
    "PreferredMaintenanceWindow": "sun:13:00-sun:13:30",
    "PubliclyAccessible": true,
    "ResizeInfo": {
        "AllowCancelResize": true,
        "ResizeType": "ClassicResize"
    },
    "RestoreStatus": {
        "CurrentRestoreRateInMegaBytesPerSecond": 15,
        "ElapsedTimeInSeconds": 120,
        "EstimatedTimeToCompletionInSeconds": 100,
        "ProgressInMegaBytes": 10,
        "SnapshotSizeInMegaBytes": 1500,
        "Status": "restoring"
    },
    "SnapshotScheduleIdentifier": "snapshotScheduleIdentifier",
    "SnapshotScheduleState": "ACTIVE",
     "VpcId": "vpc-example",
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example"
        }
    ]
```

```
}
```

AwsRoute53

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsRoute53` recursos.

AwsRoute53HostedZone

O objeto `AwsRoute53HostedZone` fornece informações sobre uma zona hospedada do Amazon Route 53, incluindo os quatro servidores de nome atribuídos à zona hospedada. Uma zona hospedada representa uma coleção de registros que podem ser gerenciados juntos, pertencentes a um único nome de domínio principal.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsRoute53HostedZone` objeto. Para ver as descrições dos `AwsRoute53HostedZone` atributos, consulte AwsRoute53 HostedZoneDetails na Referência AWS Security Hub da API.

Exemplo

```
"AwsRoute53HostedZone": {
    "HostedZone": {
        "Id": "Z06419652JEMGO9TA2XKL",
        "Name": "asff.testing",
        "Config": {
            "Comment": "This is an example comment."
        }
    },
    "NameServers": [
        "ns-470.awsdns-32.net",
        "ns-1220.awsdns-12.org",
        "ns-205.awsdns-13.com",
        "ns-1960.awsdns-51.co.uk"
    ],
    "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-
group:asfftesting:*",
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "HostedZoneId": "Z00932193AF5H180PPNZD"
        }
    },
    "Vpcs": [
```

```
        {
            "Id": "vpc-05d7c6e36bc03ea76",
            "Region": "us-east-1"
        }
    ]
}
```

AwsS3

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsS3` recursos.

AwsS3AccessPoint

O `AwsS3AccessPoint` fornece informações sobre um ponto de acesso do Amazon S3. Os pontos de acesso do S3 são endpoints de rede nomeados anexados a buckets do S3 que podem ser usados para executar operações de objeto do S3.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsS3AccessPoint` objeto. Para ver as descrições dos `AwsS3AccessPoint` atributos, consulte awSS3 AccessPointDetails na Referência da AWS Security Hub API.

Exemplo

```
"AwsS3AccessPoint": {
        "AccessPointArn": "arn:aws:s3:us-east-1:123456789012:accesspoint/asff-access-
point",
        "Alias": "asff-access-point-hrzrlukc5m36ft7okagglf3gmwluquse1b-s3alias",
        "Bucket": "DOC-EXAMPLE-BUCKET1",
        "BucketAccountId": "123456789012",
        "Name": "asff-access-point",
        "NetworkOrigin": "VPC",
        "PublicAccessBlockConfiguration": {
            "BlockPublicAcls": true,
            "BlockPublicPolicy": true,
            "IgnorePublicAcls": true,
            "RestrictPublicBuckets": true
        },
        "VpcConfiguration": {
            "VpcId": "vpc-1a2b3c4d5e6f1a2b3"
        }
}
```

AwsS3AccountPublicAccessBlock

O `AwsS3AccountPublicAccessBlock` fornece informações sobre a configuração do Amazon S3 Public Access Block para contas.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsS3AccountPublicAccessBlock` objeto. Para ver as descrições dos `AwsS3AccountPublicAccessBlock` atributos, consulte awSS3 AccountPublicAccessBlockDetails na Referência da AWS Security Hub API.

Exemplo

```
"AwsS3AccountPublicAccessBlock": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": false,
    "RestrictPublicBuckets": true
}
```

AwsS3Bucket

O objeto `AwsS3Bucket` fornece detalhes sobre um bucket do Amazon DynamoDB.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsS3Bucket` objeto. Para ver as descrições dos `AwsS3Bucket` atributos, consulte awSS3 BucketDetails na Referência da AWS Security Hub API.

Exemplo

```
"AwsS3Bucket": {
    "AccessControlList": "{\"grantSet\":null,\"grantList\":[{\"grantee\":{\"id\":
\"4df55416215956920d9d056aa8b99803a294ea221222bb668b55a8c6bca81094\",\"displayName
\":null},\"permission\":\"FullControl\"},{\"grantee\":\"AllUsers\",\"permission\":
\"ReadAcp\"},{\"grantee\":\"AuthenticatedUsers\",\"permission\":\"ReadAcp\"}",,
    "BucketLifecycleConfiguration": {
       "Rules": [
           {
               "AbortIncompleteMultipartUpload": {
                   "DaysAfterInitiation": 5
               },
               "ExpirationDate": "2021-11-10T00:00:00.000Z",
               "ExpirationInDays": 365,
               "ExpiredObjectDeleteMarker": false,
```

```
            "Filter": {
                "Predicate": {
                    "Operands": [
                        {
                            "Prefix": "tmp/",
                            "Type": "LifecyclePrefixPredicate"
                        },
                        {
                            "Tag": {
                                "Key": "ArchiveAge",
                                "Value": "9m"
                            },
                            "Type": "LifecycleTagPredicate"
                        }
                    ],
                    "Type": "LifecycleAndOperator"
                }
            },
            "ID": "Move rotated logs to Glacier",
            "NoncurrentVersionExpirationInDays": -1,
            "NoncurrentVersionTransitions": [
                {
                    "Days": 2,
                    "StorageClass": "GLACIER"
                }
            ],
            "Prefix": "rotated/",
            "Status": "Enabled",
            "Transitions": [
                {
                    "Date": "2020-11-10T00:00:00.000Z",
                    "Days": 100,
                    "StorageClass": "GLACIER"
                }
            ]
        }
    ]
},
"BucketLoggingConfiguration": {
 "DestinationBucketName": "s3serversideloggingbucket-858726136312",
 "LogFilePrefix": "buckettestreadwrite23435/"
},
"BucketName": "DOC-EXAMPLE-BUCKET1",
"BucketNotificationConfiguration": {
```

```
      "Configurations": [{
       "Destination": "arn:aws:lambda:us-east-1:123456789012:function:s3_public_write",
       "Events": [
        "s3:ObjectCreated:Put"
       ],
       "Filter": {
        "S3KeyFilter": {
         "FilterRules": [
         {
          "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.PREFIX",
          "Value": "pre"
         },
         {
          "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.SUFFIX",
          "Value": "suf"
         },
         ]
        }
       },
       "Type": "LambdaConfiguration"
      }]
     },
     "BucketVersioningConfiguration": {
      "IsMfaDeleteEnabled": true,
      "Status": "Off"
     },
     "BucketWebsiteConfiguration": {
      "ErrorDocument": "error.html",
      "IndexDocumentSuffix": "index.html",
      "RedirectAllRequestsTo": {
       "HostName": "example.com",
       "Protocol": "http"
      },
      "RoutingRules": [{
       "Condition": {
        "HttpErrorCodeReturnedEquals": "Redirected",
        "KeyPrefixEquals": "index"
          },
       "Redirect": {
        "HostName": "example.com",
        "HttpRedirectCode": "401",
        "Protocol": "HTTP",
        "ReplaceKeyPrefixWith": "string",
        "ReplaceKeyWith": "string"
```

```
      }
     }]
    },
    "CreatedAt": "2007-11-30T01:46:56.000Z",
    "ObjectLockConfiguration": {
     "ObjectLockEnabled": "Enabled",
     "Rule": {
      "DefaultRetention": {
       "Days": null,
       "Mode": "GOVERNANCE",
       "Years": 12
      },
     },
    },
    "OwnerId": "AIDACKCEVSQ6C2EXAMPLE",
    "OwnerName": "s3bucketowner",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "BlockPublicPolicy": true,
        "IgnorePublicAcls": true,
        "RestrictPublicBuckets": true,
    },
    "ServerSideEncryptionConfiguration": {
        "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "AES256",
                    "KMSMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
                }
            }
        ]
     }
}
```

AwsS3Object

O objeto `AwsS3Object` fornece informações sobre uma tabela de rotas do Amazon EC2.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsS3Object` objeto. Para ver as descrições dos `AwsS3Object` atributos, consulte awSS3 ObjectDetails na Referência da AWS Security Hub API.

Exemplo

```
"AwsS3Object": {
    "ContentType": "text/html",
    "ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
    "LastModified": "2012-04-23T18:25:43.511Z",
    "ServerSideEncryption": "aws:kms",
    "SSEKMSKeyId": "arn:aws:kms:us-west-2:123456789012:key/4dff8393-e225-4793-
a9a0-608ec069e5a7",
    "VersionId": "ws31OurgOOjH_HHllIxPE35P.MELYaYh"
}
```

AwsSageMaker

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsSageMaker` recursos.

AwsSageMakerNotebookInstance

O `AwsSageMakerNotebookInstance` objeto fornece informações sobre uma instância de SageMaker notebook da Amazon, que é uma instância computacional de aprendizado de máquina executando o aplicativo Jupyter Notebook.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsSageMakerNotebookInstance` objeto. Para ver as descrições dos `AwsSageMakerNotebookInstance` atributos, consulte AwsSageMakerNotebookInstanceDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsSageMakerNotebookInstance": {
    "DirectInternetAccess": "Disabled",
    "InstanceMetadataServiceConfiguration": {
     "MinimumInstanceMetadataServiceVersion": "1",
    },
    "InstanceType": "ml.t2.medium",
    "LastModifiedTime": "2022-09-09 22:48:32.012000+00:00",
    "NetworkInterfaceId": "eni-06c09ac2541a1bed3",
    "NotebookInstanceArn": "arn:aws:sagemaker:us-east-1:001098605940:notebook-instance/
sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm",
    "NotebookInstanceName":
 "SagemakerNotebookInstanceRootAccessDisabledComplia-8MYjcyofZiXm",
    "NotebookInstanceStatus": "InService",
```

```
    "PlatformIdentifier": "notebook-al1-v1",
    "RoleArn": "arn:aws:iam::001098605940:role/sechub-SageMaker-1-scenar-
SageMakerCustomExecution-1R0X32HGC38IW",
    "RootAccess": "Disabled",
    "SecurityGroups": [
     "sg-06b347359ab068745"
    ],
    "SubnetId": "subnet-02c0deea5fa64578e",
    "Url":
 "sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm.notebook.us-
east-1.sagemaker.aws",
    "VolumeSizeInGB": 5
}
```

AwsSecretsManager

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsSecretsManager` recursos.

AwsSecretsManagerSecret

O objeto `AwsSecretsManagerSecret` fornece detalhes sobre um segredo do Secrets Manager.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsSecretsManagerSecret` objeto. Para ver as descrições dos `AwsSecretsManagerSecret` atributos, consulte AwsSecretsManagerSecretDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsSecretsManagerSecret": {
    "RotationRules": {
        "AutomaticallyAfterDays": 30
    },
    "RotationOccurredWithinFrequency": true,
    "KmsKeyId": "kmsKeyId",
    "RotationEnabled": true,
    "RotationLambdaArn": "arn:aws:lambda:us-
west-2:777788889999:function:MyTestRotationLambda",
    "Deleted": false,
    "Name": "MyTestDatabaseSecret",
    "Description": "My test database secret"
}
```

AwsSns

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsSns` recursos.

AwsSnsTopic

O objeto `AwsSnsTopic` contém detalhes sobre um tópico do Amazon Simple Notification Service.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsSnsTopic` objeto. Para ver as descrições dos `AwsSnsTopic` atributos, consulte AwsSnsTopicDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsSnsTopic": {
    "ApplicationSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
ApplicationSuccessFeedbackRoleArn",
    "FirehoseFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseFailureFeedbackRoleArn",
    "FirehoseSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseSuccessFeedbackRoleArn",
    "HttpFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpFailureFeedbackRoleArn",
    "HttpSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpSuccessFeedbackRoleArn",
    "KmsMasterKeyId": "alias/ExampleAlias",
    "Owner": "123456789012",
    "SqsFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsFailureFeedbackRoleArn",
    "SqsSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsSuccessFeedbackRoleArn",
    "Subscription": {
         "Endpoint": "http://sampleendpoint.com",
         "Protocol": "http"
    },
    "TopicName": "SampleTopic"
}
```

AwsSqs

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsSqs` recursos.

AwsSqsQueue

O objeto `AwsSqsQueue` contém informações sobre uma fila do Amazon Simple Queue Service.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsSqsQueue` objeto. Para ver as descrições dos `AwsSqsQueue` atributos, consulte AwsSqsQueueDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsSqsQueue": {
    "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
    "KmsDataKeyReusePeriodSeconds": 60,,
    "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "QueueName": "sample-queue"
}
```

AwsSsm

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsSsm` recursos.

AwsSsmPatchCompliance

O objeto `AwsSsmPatchCompliance` fornece informações sobre o estado de um patch em uma instância com base na lista de referência de patches que foi usada para corrigir a instância.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsSsmPatchCompliance` objeto. Para ver as descrições dos `AwsSsmPatchCompliance` atributos, consulte AwsSsmPatchComplianceDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsSsmPatchCompliance": {
    "Patch": {
        "ComplianceSummary": {
            "ComplianceType": "Patch",
            "CompliantCriticalCount": 0,
            "CompliantHighCount": 0,
            "CompliantInformationalCount": 0,
            "CompliantLowCount": 0,
            "CompliantMediumCount": 0,
            "CompliantUnspecifiedCount": 461,
            "ExecutionType": "Command",
```

```
            "NonCompliantCriticalCount": 0,
            "NonCompliantHighCount": 0,
            "NonCompliantInformationalCount": 0,
            "NonCompliantLowCount": 0,
            "NonCompliantMediumCount": 0,
            "NonCompliantUnspecifiedCount": 0,
            "OverallSeverity": "UNSPECIFIED",
            "PatchBaselineId": "pb-0c5b2769ef7cbe587",
            "PatchGroup": "ExamplePatchGroup",
            "Status": "COMPLIANT"
        }
    }
}
```

AwsStepFunctions

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsStepFunctions` recursos.

AwsStepFunctionStateMachine

O objeto `AwsStepFunctionStateMachine` fornece informações sobre uma máquina de estado do AWS Step Functions , que é um fluxo de trabalho que consiste em uma série de etapas orientadas por eventos.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsStepFunctionStateMachine` objeto. Para ver as descrições dos `AwsStepFunctionStateMachine` atributos, consulte AwsStepFunctionStateMachinena Referência AWS Security Hub da API.

Exemplo

```
"AwsStepFunctionStateMachine": {
    "StateMachineArn": "arn:aws:states:us-
east-1:123456789012:stateMachine:StepFunctionsLogDisableNonCompliantResource-
fQLujTeXvwsb",
    "Name": "StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
    "Status": "ACTIVE",
    "RoleArn": "arn:aws:iam::123456789012:role/teststepfunc-
StatesExecutionRole-1PNM71RVO1UKT",
    "Type": "STANDARD",
    "LoggingConfiguration": {
```

```
        "Level": "OFF",
        "IncludeExecutionData": false
    },
    "TracingConfiguration": {
        "Enabled": false
    }
}
```

AwsWaf

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsWaf` recursos.

AwsWafRateBasedRule

O objeto `AwsWafRateBasedRule` contém detalhes sobre uma regra baseada em intervalos do AWS WAF para recursos globais. Uma regra AWS WAF baseada em taxas fornece configurações para indicar quando permitir, bloquear ou contar uma solicitação. As regras baseadas em intervalos incluem o número de solicitações recebidas durante um período especificado.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsWafRateBasedRule` objeto. Para ver as descrições dos `AwsWafRateBasedRule` atributos, consulte AwsWafRateBasedRuleDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsWafRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRateBasedRule

O objeto contém detalhes sobre uma regra baseada em intervalos do para recursos globais. Uma regra baseada em intervalos do fornece configurações para indicar quando permitir, bloquear

ou contar uma solicitação. As regras baseadas em intervalos incluem o número de solicitações recebidas durante um período especificado.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsWafRegionalRateBasedRule` objeto. Para ver as descrições dos `AwsWafRegionalRateBasedRule` atributos, consulte AwsWafRegionalRateBasedRuleDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsWafRegionalRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRule

O `AwsWafRegionalRule` objeto fornece detalhes sobre uma regra AWS WAF regional. As instruções das regra usadas para identificar as solicitações Web que você deseja permitir, bloquear ou contar.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsWafRegionalRule` objeto. Para ver as descrições dos `AwsWafRegionalRule` atributos, consulte AwsWafRegionalRuleDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsWafRegionalRule": {
    "MetricName": "SampleWAF_Rule__Metric_1",
    "Name": "bb-waf-regional-rule-not-empty-conditions-compliant",
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de95fe",
    "PredicateList": [{
        "DataId": "127d9346-e607-4e93-9286-c1296fb5445a",
```

```
        "Negated": false,
        "Type": "GeoMatch"
    }]
}
```

AwsWafRegionalRuleGroup

O objeto `AwsWafRegionalRuleGroup` fornece detalhes sobre um grupo de regras regionais do AWS WAF . Um grupo de regras é uma coleção de regras predefinidas que você adiciona a uma WebACL.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsWafRegionalRuleGroup` objeto. Para ver as descrições dos `AwsWafRegionalRuleGroup` atributos, consulte AwsWafRegionalRuleGroupDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsWafRegionalRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFClassicRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW"
        }
    }],
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
}
```

AwsWafRegionalWebAcl

`AwsWafRegionalWebAcl`fornece detalhes sobre uma lista AWS WAF regional de controle de acesso à web (Web ACL). Contém as Rules que identificam as solicitações que você deseja permitir, bloquear ou contar.

O exemplo a seguir é um exemplo de descoberta `AwsWafRegionalWebAcl` no AWS Formato do Security Finding (ASFF). Para ver as descrições dos `AwsApiGatewayV2Stage` atributos, consulte AwsWafRegionalWebAclDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsWafRegionalWebAcl": {
    "DefaultAction": "ALLOW",
    "MetricName" : "web-regional-webacl-metric-1",
    "Name": "WebACL_123",
    "RulesList": [
        {
            "Action": {
                "Type": "Block"
            },
            "Priority": 3,
            "RuleId": "24445857-852b-4d47-bd9c-61f05e4d223c",
            "Type": "REGULAR",
            "ExcludedRules": [
                {
                    "ExclusionType": "Exclusion",
                    "RuleId": "Rule_id_1"
                }
            ],
            "OverrideAction": {
                "Type": "OVERRIDE"
            }
        }
    ],
    "WebAclId": "443c76f4-2e72-4c89-a2ee-389d501c1f67"
}
```

AwsWafRule

`AwsWafRule`fornece informações sobre uma AWS WAF regra. Uma AWS WAF regra identifica as solicitações da web que você deseja permitir, bloquear ou contar.

Veja a seguir um exemplo de `AwsWafRule` descoberta no AWS Security Finding Format (ASFF). Para ver as descrições dos `AwsApiGatewayV2Stage` atributos, consulte AwsWafRuleDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsWafRule": {
    "MetricName": "AwsWafRule_Metric_1",
    "Name": "AwsWafRule_Name_1",
```

```
    "PredicateList": [{
        "DataId": "cdd225da-32cf-4773-1dc2-3bca3ed9c19c",
        "Negated": false,
        "Type": "GeoMatch"
    }],
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de953e"
}
```

AwsWafRuleGroup

`AwsWafRuleGroup`fornece informações sobre um grupo de AWS WAF regras. Um grupo de regras do AWS WAF é uma coleção de regras predefinidas que você adiciona a uma lista de controle de acesso à web (ACL da web).

Veja a seguir um exemplo de `AwsWafRuleGroup` descoberta no AWS Security Finding Format (ASFF). Para ver as descrições dos `AwsApiGatewayV2Stage` atributos, consulte AwsWafRuleGroupDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsWafRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW",
        },
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
    }]
}
```

AwsWafv2RuleGroup

O `AwsWafv2RuleGroup` objeto fornece detalhes sobre um grupo de regras AWS WAF V2.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsWafv2RuleGroup` objeto. Para ver as descrições dos `AwsWafv2RuleGroup` atributos, consulte AwsWafv2 RuleGroupDetails na Referência AWS Security Hub da API.

Exemplo

```
"AwsWafv2RuleGroup": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/wafv2rulegroupasff/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1000,
    "Description": "Resource for ASFF",
    "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "wafv2rulegroupasff",
    "Rules": [{
     "Action": {
     "Allow": {
      "CustomRequestHandling": {
       "InsertHeaders": [
        {
        "Name": "AllowActionHeader1Name",
        "Value": "AllowActionHeader1Value"
        },
        {
        "Name": "AllowActionHeader2Name",
        "Value": "AllowActionHeader2Value"
        }
       ]
      }
     },
     "Name": "RuleOne",
     "Priority": 1,
     "VisibilityConfig": {
      "CloudWatchMetricsEnabled": true,
      "MetricName": "rulegroupasff",
      "SampledRequestsEnabled": false
     }
    }],
    "VisibilityConfig": {
     "CloudWatchMetricsEnabled": true,
     "MetricName": "rulegroupasff",
     "SampledRequestsEnabled": false
    }
}
```

AwsWafWebAcl

O `AwsWafWebAcl` objeto fornece detalhes sobre uma AWS WAF Web ACL.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsWafWebAcl` objeto. Para ver as descrições dos `AwsWafWebAcl` atributos, consulte AwsWafWebAclDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsWafWebAcl": {
    "DefaultAction": "ALLOW",
    "Name": "MyWafAcl",
    "Rules": [
        {
            "Action": {
                "Type": "ALLOW"
            },
            "ExcludedRules": [
                {
                    "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98"
                }
            ],
            "OverrideAction": {
                "Type": "NONE"
            },
            "Priority": 1,
            "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98",
            "Type": "REGULAR"
        }
    ],
    "WebAclId": "waf-1234567890"
}
```

AwsWafv2WebAcl

O `AwsWafv2WebAcl` objeto fornece detalhes sobre uma Web AWS WAF ACL V2.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsWafv2WebAcl` objeto. Para ver as descrições dos `AwsWafv2WebAcl` atributos, consulte AwsWafv2 WebAclDetails na Referência AWS Security Hub da API.

Exemplo

```
"AwsWafv2WebAcl": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/WebACL-RoaD4QexqSxG/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
    "Capacity": 1326,
    "CaptchaConfig": {
     "ImmunityTimeProperty": {
      "ImmunityTime": 500
     }
    },
    "DefaultAction": {
     "Block": {}
    },
    "Description": "Web ACL for JsonBody testing",
    "ManagedbyFirewallManager": false,
    "Name": "WebACL-RoaD4QexqSxG",
    "Rules": [{
     "Action": {
      "RuleAction": {
       "Block": {}
      }
     },
     "Name": "TestJsonBodyRule",
     "Priority": 1,
     "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "JsonBodyMatchMetric"
     }
    }],
    "VisibilityConfig": {
     "SampledRequestsEnabled": true,
     "CloudWatchMetricsEnabled": true,
     "MetricName": "TestingJsonBodyMetric"
    }
}
```

AwsXray

Veja a seguir exemplos do formato de descoberta de AWS segurança para `AwsXray` recursos.

AwsXrayEncryptionConfig

O `AwsXrayEncryptionConfig` objeto contém informações sobre a configuração de criptografia do AWS X-Ray.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `AwsXrayEncryptionConfig` objeto. Para ver as descrições dos `AwsXrayEncryptionConfig` atributos, consulte AwsXrayEncryptionConfigDetailsna Referência AWS Security Hub da API.

Exemplo

```
"AwsXRayEncryptionConfig":{
    "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
    "Status": "UPDATING",
    "Type":"KMS"
}
```

Container

Detalhes do contêiner relacionados a uma descoberta.

O exemplo a seguir mostra o AWS Security Finding Format (ASFF) do `Container` objeto. Para ver as descrições dos `Container` atributos, consulte ContainerDetailsna Referência AWS Security Hub da API.

Exemplo

```
"Container": {
    "ContainerRuntime": "docker",
    "ImageId": "image12",
    "ImageName": "1111111/
knotejs@sha256:372131c9fef111111111111115f4ed3ea5f9dce4dc3bd34ce21846588a3",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "Name": "knote",
    "Privileged": true,
    "VolumeMounts": [{
        "Name": "vol-03909e9",
        "MountPath": "/mnt/etc"
    }]
}
```

Other

O objeto`Other` permite fornecer campos e valores personalizados. Use o subcampo `Other` nos seguintes casos.

- O tipo de recurso não tem um subcampo correspondente. Para fornecer detalhes para o recurso, use o subcampo `Other`.
- O subcampo do tipo de recurso não inclui todos os campos que você deseja preencher. Nesse caso, use o subcampo do tipo de recurso para preencher os campos disponíveis. Use o objeto `Other` para preencher os atributos que não estão no objeto específico do tipo.
- O tipo de recurso não é um dos tipos fornecidos. Nesse caso, defina `Resource.Type` como `Other` e use o subcampo `Other` para preencher os detalhes.

Tipo: mapa de até 50 pares de chave-valor

Cada par de chave-valor deve atender aos seguintes requisitos.

- A chave deve conter menos de 128 caracteres.
- O valor deve conter menos de 1.024 caracteres.

Insights no AWS Security Hub

Um insight do AWS Security Hub é uma coleção de descobertas relacionadas. Identifica uma área de segurança que requer atenção e intervenção. Por exemplo, um insight pode indicar instâncias do EC2 que são objeto de descobertas que detectam práticas de segurança inadequadas. Um insight reúne as descobertas de provedores de busca.

Cada insight é definido por uma instrução group by e filtros opcionais. A instrução group by indica como agrupar as descobertas correspondentes e identifica o tipo de item ao qual o insight se aplica. Por exemplo, se um insight for agrupado por identificador de recurso, ele produzirá uma lista de identificadores de recursos. Os filtros opcionais identificam as descobertas correspondentes para o insight. Por exemplo, talvez você queira ver apenas descobertas de provedores específicos ou descobertas que são associadas a tipos específicos de recursos.

O Security Hub oferece vários insights gerenciados internos. Você não pode modificar ou excluir insights gerenciados.

Para rastrear problemas de segurança que são exclusivos do seu ambiente da AWS e uso, você pode criar insights personalizados.

Um insight só retornará resultados se você tiver ativado integrações ou padrões que produzem descobertas correspondentes. Por exemplo, o insight gerenciado 29. Principais recursos por contagens de verificações de CIS com falha retornarão resultados somente se você ativar o padrão de segurança CIS AWS Foundations.

Tópicos

Visualizar e filtrar a lista de insights

A página Insights exibe a lista de insights disponíveis.

Por padrão, a lista exibe insights gerenciados e personalizados. Para filtrar a lista de insights com base no tipo de insight, escolha o tipo no menu suspenso ao lado do campo de filtro.

- Para exibir todos os insights disponíveis, escolha Todos os insights. Esta é a opção padrão.
- Para exibir somente insights gerenciados, escolha insights gerenciados do Security Hub.
- Para exibir somente insights personalizados, escolha Insights personalizados.

Você também pode filtrar a lista de insights com base no texto no nome do insight.

No campo de filtro, digite o texto a ser usado para filtrar a lista. O filtro não faz distinção entre letras maiúsculas de minúsculas. O filtro procura insights que contenham o texto em qualquer lugar no nome do insight.

Visualizar e tomar medidas em resultados e descobertas de insight

Para cada insight, o AWS Security Hub primeiro determina as descobertas que correspondem aos critérios do filtro e, em seguida, usa o atributo de agrupamento para agrupar as descobertas correspondentes.

Na página Insights do console, você pode exibir e agir sobre os resultados e as descobertas.

Se você habilitar a agregação entre regiões, na região de agregação, os resultados dos insights gerenciados incluirão descobertas da região de agregação e das regiões vinculadas. Para resultados de insights personalizados, se o insight não for filtrado por região, os resultados incluirão descobertas da região de agregação e regiões vinculadas.

Em outras regiões, os resultados do insight são somente para aquela região.

Para obter informações sobre como configurar a agregação entre regiões, consulte. Agregação entre regiões

Visualizar e tomar medidas em resultados de insight (console)

Os resultados do insight consistem em uma lista agrupada dos resultados para o insight. Por exemplo, se o insight for agrupado por identificadores de recurso, os resultados de insight serão a lista de identificadores de recurso. Cada item na lista de resultados indica o número de descobertas correspondentes para esse item.

Observe que se as descobertas forem agrupadas por identificador de recurso ou tipo de recurso, os resultados incluirão todos os recursos nas descobertas correspondentes. Isso inclui recursos que têm um tipo diferente do tipo de recurso especificado nos critérios de filtro. Por exemplo, um insight

identifica descobertas associadas aos buckets do S3. Se uma descoberta correspondente contiver um recurso de bucket do S3 e um recurso de chave de acesso do IAM, os resultados do insight listarão ambos os recursos.

A lista de resultados é classificada do maior para o menor número de descobertas correspondentes.

O Security Hub só pode exibir 100 resultados. Se houver mais de 100 valores de agrupamento, você verá somente os 100 primeiros.

Além da lista de resultados, os resultados do insight exibem um conjunto de gráficos resumindo o número de descobertas correspondentes para os seguintes atributos.

- Rótulo de gravidade – número de descobertas para cada rótulo de gravidade
- Conta da AWS ID — Os cinco principais IDs de conta para as descobertas correspondentes
- Tipo de recurso – cinco principais tipos de recurso para as descobertas correspondentes
- ID do recurso – cinco principais IDs de recurso para as descobertas correspondentes
- Nome do produto – cinco principais provedores para as descobertas correspondentes

Se você configurou ações personalizadas, poderá enviar resultados selecionados para uma ação personalizada. A ação deve estar associada a uma CloudWatch regra para o tipo de `Security Hub Insight Results` evento. Consulte the section called “Resposta e remediação automatizadas”.

Se você não configurou ações personalizadas, o menu Ações será desativado.

Como exibir e tomar medidas na lista de resultados de insight

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Insights.
3. Para exibir a lista de resultados de insight, escolha o nome do insight.
4. Marque a caixa de seleção para cada resultado a ser enviado para a ação personalizada.
5. No menu Actions (Ações), escolha a ação personalizada.

Visualizando resultados de insights (API do Security Hub, AWS CLI)

Para visualizar os resultados do insight, você pode usar uma chamada de API ou o AWS Command Line Interface.

Para ver os resultados do insight (API do Security Hub, AWS CLI)

- API do Security Hub – use a operação API `GetInsightResults`. Para identificar o insight para o qual retornar resultados, você precisa do ARN do insight. Para obter os ARNs de insights para insights personalizados, use a operação `GetInsights` .
- AWS CLI – na linha de comando, execute o comando `get-insight-results`.

```
aws securityhub get-insight-results --insight-arn <insight ARN>
```

Exemplo:

```
aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Visualizar descobertas para um resultado de insight (console)

Na lista de resultados de insight, você pode exibir a lista de descobertas para cada resultado.

Como exibir e tomar medidas sobre as descobertas de insight

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Insights.
3. Para exibir a lista de resultados de insight, escolha o nome do insight.
4. Para exibir a lista de descobertas para um resultado de insight, escolha o item na lista de resultados.

A lista de descobertas mostra as descobertas ativas para o resultado do insight selecionado com um status de fluxo de trabalho de `NEW` ou `NOTIFIED`.

Na lista de descobertas, é possível executar as ações a seguir.

- Alterar os filtros e o agrupamento da lista
- Visualizar detalhes de descobertas individuais
- Atualizar o status do fluxo de trabalho das descobertas
- Enviar descobertas para ações personalizadas

Insights gerenciados

O Security Hub AWS fornece vários insights gerenciados.

Não é possível editar ou excluir insights gerenciados do Security Hub. É possível visualizar e tomar medidas sobre os resultados e as descobertas do insight. Você também pode usar um insight gerenciado como base para um novo insight personalizado.

Assim como acontece com todos os insights, um insight gerenciado só retornará resultados se você tiver habilitado integrações de produtos ou padrões de segurança que possam produzir descobertas correspondentes.

Para insights agrupados por identificador de recurso, os resultados incluem os identificadores de todos os recursos nas descobertas correspondentes. Isso inclui recursos que têm um tipo diferente do tipo de recurso nos critérios de filtro. Por exemplo, o insight 2 identifica descobertas associadas aos buckets do Amazon S3. Se uma descoberta correspondente contiver um recurso de bucket do S3 e um recurso de chave de acesso do IAM, os resultados do insight incluirão os dois recursos.

O Security Hub oferece os seguintes insights gerenciados:

1. Recursos da AWS com a maioria das descobertas

   ARN: `arn:aws:securityhub:::insight/securityhub/default/1`

   Agrupado por: identificador de recurso

   Filtros de descoberta:

   - O estado do registro é `ACTIVE`
   - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

2. Os buckets do S3 com permissões de gravação ou leitura públicas

   ARN: `arn:aws:securityhub:::insight/securityhub/default/10`

   Agrupado por: identificador de recurso

   Filtros de descoberta:

   - Tipo começa com `Effects/Data Exposure`
   - O tipo de recurso é `AwsS3Bucket`
   - O estado do registro é `ACTIVE`

- O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

3. AMIs que geram a maioria das descobertas

   ARN: `arn:aws:securityhub:::insight/securityhub/default/3`

   Agrupado por: ID da imagem da instância EC2

   Filtros de descoberta:

   - O tipo de recurso é `AwsEc2Instance`
   - O estado do registro é `ACTIVE`
   - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

4. As instâncias do EC2 envolvidas em Táticas, Técnicas e Procedimentos (TTPs) conhecidas

   ARN: `arn:aws:securityhub:::insight/securityhub/default/14`

   Agrupado por: ID do recurso

   Filtros de descoberta:

   - Tipo começa com `TTPs`
   - O tipo de recurso é `AwsEc2Instance`
   - O estado do registro é `ACTIVE`
   - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

5. Entidades principais da AWS com atividade suspeita de chave de acesso

   ARN: `arn:aws:securityhub:::insight/securityhub/default/9`

   Agrupado por: nome da entidade principal da chave de acesso do IAM

   Filtros de descoberta:

   - O tipo de recurso é `AwsIamAccessKey`
   - O estado do registro é `ACTIVE`
   - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

6. Instâncias de recursos da AWS que não atendem aos padrões de segurança e às práticas recomendadas

   ARN: `arn:aws:securityhub:::insight/securityhub/default/6`

   Agrupado por: ID do recurso

Filtros de descoberta:

- O tipo é `Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices`
- O estado do registro é `ACTIVE`
- O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

7. Recursos da AWS associados a exfiltração de dados em potencial

   ARN: `arn:aws:securityhub:::insight/securityhub/default/7`

   Agrupado por: ID do recurso

   Filtros de descoberta:

   - O tipo começa com Effects/Exfiltração de dados/
   - O estado do registro é `ACTIVE`
   - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

8. Recursos da AWS associados ao consumo de recursos não autorizado

   ARN: `arn:aws:securityhub:::insight/securityhub/default/8`

   Agrupado por: ID do recurso

   Filtros de descoberta:

   - Tipo começa com `Effects/Resource Consumption`
   - O estado do registro é `ACTIVE`
   - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

9. Buckets do S3 que não atendem aos padrões de segurança e às práticas recomendadas

   ARN: `arn:aws:securityhub:::insight/securityhub/default/11`

   Agrupado por: ID do recurso

   Filtros de descoberta:

   - O tipo de recurso é `AwsS3Bucket`
   - O tipo é `Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices`
   - O estado do registro é `ACTIVE`

- O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

10. Os buckets do S3 com dados confidenciais

    ARN: `arn:aws:securityhub:::insight/securityhub/default/12`

    Agrupado por: ID do recurso

    Filtros de descoberta:

    - O tipo de recurso é `AwsS3Bucket`
    - Tipo começa com `Sensitive Data Identifications/`
    - O estado do registro é `ACTIVE`
    - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

11. Credenciais que podem ter vazado

    ARN: `arn:aws:securityhub:::insight/securityhub/default/13`

    Agrupado por: ID do recurso

    Filtros de descoberta:

    - Tipo começa com `Sensitive Data Identifications/Passwords/`
    - O estado do registro é `ACTIVE`
    - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

12. As instâncias do EC2 que possuem patches de segurança ausentes para vulnerabilidades importantes

    ARN: `arn:aws:securityhub:::insight/securityhub/default/16`

    Agrupado por: ID do recurso

    Filtros de descoberta:

    - Tipo começa com `Software and Configuration Checks/Vulnerabilities/CVE`
    - O tipo de recurso é `AwsEc2Instance`
    - O estado do registro é `ACTIVE`
    - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

13. As instâncias do EC2 com comportamento geral incomum

    ARN: `arn:aws:securityhub:::insight/securityhub/default/17`

Agrupado por: ID do recurso

Filtros de descoberta:

- Tipo começa com `Unusual Behaviors`
- O tipo de recurso é `AwsEc2Instance`
- O estado do registro é `ACTIVE`
- O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

14. Instâncias de EC2 com portas acessíveis pela Internet

ARN: `arn:aws:securityhub:::insight/securityhub/default/18`

Agrupado por: ID do recurso

Filtros de descoberta:

- Tipo começa com `Software and Configuration Checks/AWS Security Best Practices/Network Reachability`
- O tipo de recurso é `AwsEc2Instance`
- O estado do registro é `ACTIVE`
- O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

15. Instâncias de EC2 que não atendem aos padrões de segurança e às práticas recomendadas

ARN: `arn:aws:securityhub:::insight/securityhub/default/19`

Agrupado por: ID do recurso

Filtros de descoberta:

- O tipo começa com um dos seguintes:
  - `Software and Configuration Checks/Industry and Regulatory Standards/`
  - `Software and Configuration Checks/AWS Security Best Practices`
- O tipo de recurso é `AwsEc2Instance`
- O estado do registro é `ACTIVE`
- O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

16. Instâncias de EC2 que estão abertas à Internet

ARN: `arn:aws:securityhub:::insight/securityhub/default/21`

Agrupado por: ID do recurso

Filtros de descoberta:

- Tipo começa com `Software and Configuration Checks/AWS Security Best Practices/Network Reachability`
- O tipo de recurso é `AwsEc2Instance`
- O estado do registro é `ACTIVE`
- O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

17. As instâncias do EC2 associadas ao reconhecimento de adversários

    ARN: `arn:aws:securityhub:::insight/securityhub/default/22`

    Agrupado por: ID do recurso

    Filtros de descoberta:

    - O tipo começa com TTPs/Descoberta/Recon
    - O tipo de recurso é `AwsEc2Instance`
    - O estado do registro é `ACTIVE`
    - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

18. Recursos da AWS associados a malware

    ARN: `arn:aws:securityhub:::insight/securityhub/default/23`

    Agrupado por: ID do recurso

    Filtros de descoberta:

    - O tipo começa com um dos seguintes:
      - `Effects/Data Exfiltration/Trojan`
      - `TTPs/Initial Access/Trojan`
      - `TTPs/Command and Control/Backdoor`
      - `TTPs/Command and Control/Trojan`
      - `Software and Configuration Checks/Backdoor`
      - `Unusual Behaviors/VM/Backdoor`
    - O estado do registro é `ACTIVE`
    - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

19. Recursos da AWS associados a problemas de criptomoedas

    ARN: `arn:aws:securityhub:::insight/securityhub/default/24`

    Agrupado por: ID do recurso

    Filtros de descoberta:

    - O tipo começa com um dos seguintes:
      - `Effects/Resource Consumption/Cryptocurrency`
      - `TTPs/Command and Control/CryptoCurrency`
    - O estado do registro é `ACTIVE`
    - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`
20. Recursos da AWS com tentativas de acesso não autorizado

    ARN: `arn:aws:securityhub:::insight/securityhub/default/25`

    Agrupado por: ID do recurso

    Filtros de descoberta:

    - O tipo começa com um dos seguintes:
      - `TTPs/Command and Control/UnauthorizedAccess`
      - `TTPs/Initial Access/UnauthorizedAccess`
      - `Effects/Data Exfiltration/UnauthorizedAccess`
      - `Unusual Behaviors/User/UnauthorizedAccess`
      - `Effects/Resource Consumption/UnauthorizedAccess`
    - O estado do registro é `ACTIVE`
    - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`
21. Indicadores de ameaça Intel com o maior número de acertos na última semana

    ARN: `arn:aws:securityhub:::insight/securityhub/default/26`

    Filtros de descoberta:

    - Criado nos últimos 7 dias
22. Principais contas por contagem de descobertas

    ARN: `arn:aws:securityhub:::insight/securityhub/default/27`

Agrupado por: ID da Conta da AWS

Filtros de descoberta:

- O estado do registro é `ACTIVE`
- O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

23. Principais produtos por contagem de descobertas

    ARN: `arn:aws:securityhub:::insight/securityhub/default/28`

    Agrupado por: Nome do produto

    Filtros de descoberta:

    - O estado do registro é `ACTIVE`
    - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

24. Gravidade por contagem de descobertas

    ARN: `arn:aws:securityhub:::insight/securityhub/default/29`

    Agrupado por: Rótulo de gravidade

    Filtros de descoberta:

    - O estado do registro é `ACTIVE`
    - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

25. Principais buckets do S3 por contagem de descobertas

    ARN: `arn:aws:securityhub:::insight/securityhub/default/30`

    Agrupado por: ID do recurso

    Filtros de descoberta:

    - O tipo de recurso é `AwsS3Bucket`
    - O estado do registro é `ACTIVE`
    - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

26. Principais instâncias de EC2 por contagem de descobertas

    ARN: `arn:aws:securityhub:::insight/securityhub/default/31`

    Agrupado por: ID do recurso

Filtros de descoberta:

- O tipo de recurso é `AwsEc2Instance`
- O estado do registro é `ACTIVE`
- O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

27. Principais AMIs por contagem de descobertas

    ARN: `arn:aws:securityhub:::insight/securityhub/default/32`

    Agrupado por: ID da imagem da instância EC2

    Filtros de descoberta:

    - O tipo de recurso é `AwsEc2Instance`
    - O estado do registro é `ACTIVE`
    - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

28. Principais usuários do IAM por contagem de descobertas

    ARN: `arn:aws:securityhub:::insight/securityhub/default/33`

    Agrupado por: ID da chave de acesso do IAM

    Filtros de descoberta:

    - O tipo de recurso é `AwsIamAccessKey`
    - O estado do registro é `ACTIVE`
    - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

29. Principais recursos por contagem de verificações de CIS com falha

    ARN: `arn:aws:securityhub:::insight/securityhub/default/34`

    Agrupado por: ID do recurso

    Filtros de descoberta:

    - O ID do gerador começa com `arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule`
    - Atualizado no último dia
    - O status de conformidade é `FAILED`

- O estado do registro é `ACTIVE`
- O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

30. Principais integrações por contagem de descobertas

    ARN: `arn:aws:securityhub:::insight/securityhub/default/35`

    Agrupado por: ARN do produto

    Filtros de descoberta:

    - O estado do registro é `ACTIVE`
    - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

31. Recursos com as verificações de segurança com mais falhas

    ARN: `arn:aws:securityhub:::insight/securityhub/default/36`

    Agrupado por: ID do recurso

    Filtros de descoberta:

    - Atualizado no último dia
    - O status de conformidade é `FAILED`
    - O estado do registro é `ACTIVE`
    - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

32. Usuários do IAM com atividades suspeitas

    ARN: `arn:aws:securityhub:::insight/securityhub/default/37`

    Agrupado por: Usuário do IAM

    Filtros de descoberta:

    - O tipo de recurso é `AwsIamUser`
    - O estado do registro é `ACTIVE`
    - O status do fluxo de trabalho é `NEW` ou `NOTIFIED`

33. Recursos com a maioria das descobertas do AWS Health

    ARN: `arn:aws:securityhub:::insight/securityhub/default/38`

    Agrupado por: ID do recurso

Filtros de descoberta:

- `ProductName` igual a `Health`

34. Recursos com a maioria das descobertas do AWS Config

    ARN: `arn:aws:securityhub:::insight/securityhub/default/39`

    Agrupado por: ID do recurso

    Filtros de descoberta:

    - `ProductName` igual a `Config`

35. Aplicações com mais descobertas

    ARN: `arn:aws:securityhub:::insight/securityhub/default/40`

    Agrupado por: ResourceApplicationArn

    Filtros de descoberta:

    - `RecordState` igual a `ACTIVE`
    - `Workflow.Status` é igual a `NEW` ou `NOTIFIED`

Insights personalizados

Além dos insights gerenciados do AWS Security Hub, você pode criar insights personalizados para rastrear problemas e recursos específicos do seu ambiente. Os insights personalizados oferecem uma forma de monitorar um subconjunto organizado de problemas.

Aqui estão alguns exemplos de insights personalizados que podem ser úteis configurar:

- Se você tiver uma conta de administrador, pode configurar uma visão personalizada para rastrear descobertas críticas e de alta gravidade que estão afetando as contas dos membros.
- Se você confia em um serviço integrado da AWS específico, pode configurar um insight personalizado para rastrear descobertas críticas e de alta gravidade desse serviço.
- Se você depende de uma integração de terceiros, pode configurar um insight personalizado para rastrear descobertas críticas e de alta gravidade desse produto integrado.

Você pode criar insights personalizados completamente novos ou começar a partir de um insight personalizado ou gerenciado existente.

Cada insight é configurado com as seguintes opções.

- Atributo de agrupamento: o atributo de agrupamento determina os itens que são exibidos na lista de resultados do insight. Por exemplo, se o atributo de agrupamento for Nome do produto, os resultados do insight exibirão o número de descobertas associadas a cada provedor de descoberta.
- Filtros opcionais: os filtros opcionais reduzem as descobertas correspondentes para o insight.

  Ao consultar suas descobertas, o Security Hub aplica a lógica Booleana E ao conjunto de filtros. Em outras palavras, uma descoberta só será correspondente se corresponder a todos os filtros fornecidos. Por exemplo, se os filtros forem “O nome do produto é GuardDuty" e “O tipo de recurso é `AwsS3Bucket`”,as descobertas correspondentes deverão corresponder a esses dois critérios.

  No entanto, o Security Hub aplica a lógica Booleana OU a filtros que usam o mesmo atributo, mas valores diferentes. Por exemplo, se os filtros forem “O nome do produto é GuardDuty" e “O nome do produto é Amazon Inspector", uma descoberta será correspondente se tiver sido gerada por GuardDuty ou Amazon Inspector.

Observe que, se você usar o identificador ou o tipo de recurso como atributo de agrupamento, os resultados do insight incluirão todos os recursos que estão nas descobertas correspondentes. A lista não está limitada aos recursos que correspondem a um filtro de tipo de recurso. Por exemplo, um insight identifica as descobertas associadas aos buckets do S3 e agrupa essas descobertas por identificador de recurso. uma descoberta correspondente contiver um recurso de bucket do S3 e um recurso de chave de acesso do IAM. Os resultados do insight incluem ambos os recursos.

Criar um insight personalizado (console)

No console, você pode criar um insight completamente novo.

Criar um insight personalizado

1. Abra o AWS console do Security Hub em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Insights.
3. Escolha Criar insight.
4. Para selecionar o atributo de agrupamento do insight:
   a. Escolha a caixa de pesquisa para exibir as opções de filtro.
   b. Escolha Agrupar por.

c. Selecione o atributo a ser usado para agrupar as descobertas que são associadas a esse insight.

d. Escolha Aplicar.

5. (Opcional) Escolha quaisquer filtros adicionais a serem usados para esse insight. Para cada filtro, defina o critério de filtro e escolha Aplicar.
6. Escolha Criar insight.
7. Insira um Nome do insight e escolha Criar insight.

Criar uma visão personalizada (programática)

Escolha seu método preferido e siga as etapas abaixo para criar programaticamente uma visão personalizada no Security Hub. Você pode especificar filtros para restringir a coleção de descobertas no insight a um subconjunto específico.

As guias a seguir incluem instruções em alguns idiomas para criar um insight personalizado. Para obter suporte em outros idiomas, consulte Ferramentas para desenvolver em AWS.

Security Hub API

1. Execute a `CreateInsight`operação.
2. Preencha o `Name` parâmetro com um nome para seu insight personalizado.
3. Preencha o `Filters` parâmetro para especificar quais descobertas devem ser incluídas no insight.
4. Preencha o `GroupByAttribute` parâmetro para especificar quais atributos são ousados para agrupar as descobertas incluídas no insight.
5. Opcionalmente, preencha o parâmetro `SortCriteria` para classificar as descobertas por um campo específico.

Se você habilitou a agregação entre regiões e chamou essa API da região de agregação, o insight se aplica às descobertas correspondentes na agregação e nas regiões vinculadas.

AWS CLI

1. Na linha de comando, execute o comando `create-insight`.
2. Preencha o `name` parâmetro com um nome para seu insight personalizado.

3. Preencha o `filters` parâmetro para especificar quais descobertas devem ser incluídas no insight.
4. Preencha o `group-by-attribute` parâmetro para especificar quais atributos são ousados para agrupar as descobertas incluídas no insight.

Se você habilitou a agregação entre regiões e executou esse comando na região de agregação, o insight se aplica às descobertas correspondentes da agregação e das regiões vinculadas.

```
aws securityhub create-insight --name <insight name> --filters <filter values> --
group-by-attribute <attribute name>
```

Exemplo

```
aws securityhub create-insight --name "Critical role findings" --filters
 '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}],
 "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-
attribute "ResourceId"
```

PowerShell

1. Use o cmdlet `New-SHUBInsight`.
2. Preencha o `Name` parâmetro com um nome para seu insight personalizado.
3. Preencha o `Filter` parâmetro para especificar quais descobertas devem ser incluídas no insight.
4. Preencha o `GroupByAttribute` parâmetro para especificar quais atributos são ousados para agrupar as descobertas incluídas no insight.

Se você habilitou a agregação entre regiões e usa esse cmdlet desde a região de agregação, o insight se aplica às descobertas correspondentes da agregação e das regiões vinculadas.

Exemplo

```
$Filter = @{
    AwsAccountId = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "XXX"
    }
```

```
    ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = 'FAILED'
    }
}
New-SHUBInsight -Filter $Filter -Name TestInsight -GroupByAttribute ResourceId
```

Modificar um insight personalizado (console)

Você pode modificar um insight personalizado existente para alterar o valor de agrupamento e os filtros. Depois de fazer as alterações, você pode salvar as atualizações no insight original ou salvar a versão atualizada como um novo insight.

Para modificar um insight

1. Abra o AWS console do Security Hub em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Insights.
3. Escolha o insight personalizado a ser modificado.
4. Edite a configuração do insight, se necessário.
   - Para alterar o atributo usado para agrupar descobertas no insight:
     a. Para remover o agrupamento existente, escolha o X ao lado da configuração Agrupar por.
     b. Escolha a caixa Pesquisar.
     c. Selecione o atributo a ser usado para agrupamento.
     d. Escolha Aplicar.
   - Para remover um filtro do insight, escolha o X circulado ao lado do filtro.
   - Para adicionar um filtro ao insight:
     a. Escolha a caixa Pesquisar.
     b. Selecione o atributo e o valor a serem usados como filtro.
     c. Escolha Aplicar.
5. Ao concluir as atualizações, escolha Salvar insight.
6. Quando solicitado, siga um destes procedimentos:
   - Para substituir um insight existente para refletir as alterações, escolha Atualizar ***<Insight_Name>*** e então escolha Salvar insight.

- Para criar um insight com as atualizações, escolha Salvar novo insight. Insira um Nome de insight e então escolha Salvar insight.

Modificar um insight personalizado (programático)

Para modificar um insight personalizado, escolha seu método preferido e siga as instruções.

Security Hub API

1. Execute a `UpdateInsight`operação.
2. Para identificar o insight personalizado, forneça o nome do recurso da Amazon (ARN) do insight. Para obter o ARN de um insight personalizado, execute a `GetInsights`operação.
3. Atualizar os parâmetros `Name`, `Filters`, e `GroupByAttribute` conforme necessário.

AWS CLI

1. Na linha de comando, execute o comando `update-insight`.
2. Para identificar o insight personalizado, forneça o nome do recurso da Amazon (ARN) do insight. Para obter o ARN de um insight personalizado, execute o comando `get-insights`.
3. Atualizar os parâmetros `name`, `filters`, e `group-by-attribute` conforme necessário.

```
aws securityhub update-insight --insight-arn <insight ARN> [--name <new name>] [--
filters <new filters>] [--group-by-attribute <new grouping attribute>]
```

Exemplo

```
aws securityhub update-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" --filters '{"ResourceType": [{ "Comparison": "EQUALS", "Value":
 "AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "HIGH"}]}' --
name "High severity role findings"
```

PowerShell

1. Use o cmdlet `Update-SHUBInsight`.
2. Para identificar o insight personalizado, forneça o nome do recurso da Amazon (ARN) do insight. Para obter o ARN de um insight personalizado, use o cmdlet `Get-SHUBInsight`.

3. Atualizar os parâmetros `Name`, `Filter`, e `GroupByAttribute` conforme necessário.

Exemplo

```
$Filter = @{
    ResourceType = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "AwsIamRole"
    }
    SeverityLabel = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "HIGH"
    }
}

Update-SHUBInsight -InsightArn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" -Filter $Filter -Name "High severity role findings"
```

Criar um novo insight personalizado com base em um insight gerenciado (console)

Você não pode salvar alterações ou excluir um insight gerenciado. Você pode usar um insight gerenciado como base para um novo insight personalizado.

Como criar um novo insight personalizado com base em um insight gerenciado

1. Abra o AWS console do Security Hub em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Insights.
3. Escolha o insight gerenciado no qual trabalhar.
4. Edite a configuração do insight, se necessário.
   - Para alterar o atributo usado para agrupar descobertas no insight:
     a. Para remover o agrupamento existente, escolha o X ao lado da configuração Agrupar por.
     b. Escolha a caixa Pesquisar.
     c. Selecione o atributo a ser usado para agrupamento.
     d. Escolha Aplicar.

- Para remover um filtro do insight, escolha o X circulado ao lado do filtro.
- Para adicionar um filtro ao insight:
  a. Escolha a caixa Pesquisar.
  b. Selecione o atributo e o valor a serem usados como filtro.
  c. Escolha Aplicar.

5. Quando as atualizações estiverem concluídas, escolha Criar insight.
6. Quando solicitado, insira um Nome de insight e então escolha Criar insight .

Excluir um insight personalizado (console)

Quando você não quiser mais um insight personalizado, poderá excluí-lo. Você não pode excluir insights gerenciados.

Para excluir um insight personalizado

1. Abra o console do Security Hub AWS em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Insights.
3. Localize o insight personalizado a ser excluído.
4. Para esse insight, escolha o ícone de mais opções (os três pontos no canto superior direito do cartão).
5. Escolha Excluir.

Excluir um insight personalizado (programático)

Para excluir um insight personalizado, escolha seu método preferido e siga as instruções.

Security Hub API

1. Execute a `DeleteInsight`operação.
2. Para identificar o insight personalizado a ser excluído, forneça o ARN do insight. Para obter o ARN de um insight personalizado, execute a `GetInsights`operação.

AWS CLI

1. Na linha de comando, execute o comando `delete-insight`.

2. Para identificar o insight personalizado, forneça o ARN do insight. Para obter o ARN de um insight personalizado, execute o comando `get-insights`.

```
aws securityhub delete-insight --insight-arn <insight ARN>
```

Exemplo

```
aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

PowerShell

1. Use o cmdlet `Remove-SHUBInsight`.
2. Para identificar o insight personalizado, forneça o ARN do insight. Para obter o ARN de um insight personalizado, use o cmdlet `Get-SHUBInsight`.

Exemplo

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Automações

As automações do Security Hub podem ajudá-lo a modificar e corrigir rapidamente as descobertas com base em suas especificações.

O Security Hub oferece suporte atualmente a dois tipos de automações:

- Regras de automação — atualize e suprima automaticamente as descobertas quase em tempo real com base nos critérios definidos por você.
- Resposta e remediação automatizadas — Crie regras personalizadas do EventBridge que definam ações automáticas a serem tomadas em relação a descobertas e insights específicos.

As regras de automação se aplicam antes das regras do EventBridge. Ou seja, as regras de automação são acionadas e atualizam uma descoberta antes que ela seja enviada ao EventBridge. As regras do EventBridge então se aplicam à descoberta atualizada.

Ao configurar automações para controles de segurança, recomendamos filtrar com base no ID do controle, e não no título ou na descrição. Embora o Security Hub ocasionalmente atualize títulos e descrições de controle, os IDs de controle permanecem os mesmos.

Tópicos

Regras de automação

As regras de automação podem ser usadas para atualizar automaticamente as descobertas no Security Hub. À medida que as descobertas são recebidas, o Security Hub pode aplicar diversas ações de regras, como suprimir descobertas, alterar a gravidade e adicionar notas às descobertas. Essas ações de regra entram em vigor quando as descobertas correspondem aos critérios especificados, como o ID da conta ou recurso à qual a descoberta está associada ou seu título.

Os exemplos de casos de uso de regras de automação incluem:

- Elevar a gravidade de uma descoberta para `CRITICAL` se o ID do recurso da descoberta se referir a um recurso crítico para os negócios.

- Elevar a gravidade de uma descoberta de `HIGH` para `CRITICAL` se a descoberta afetar recursos em contas de produção específicas.
- Atribuir descobertas específicas que tenham um status de fluxo de trabalho com gravidade de `INFORMATIONAL` a `SUPPRESSED`.

As regras de automação podem ser usadas para atualizar campos de descoberta selecionados no AWSFormato do Security Finding (ASFF). As regras se aplicam às novas descobertas e às descobertas atualizadas.

É possível criar uma regra personalizada do zero ou usar um modelo de regra fornecido pelo Security Hub. Se você usar um modelo de regra, poderá modificá-lo conforme necessário para seu caso de uso.

Como as regras de automação funcionam

O administrador do Security Hub pode criar uma regra de automação definindo critérios de regras. Quando uma descoberta corresponde aos critérios definidos, o Security Hub aplica a ação da regra a ela. Para obter mais informações sobre critérios e ações disponíveis, consulte Critérios de regras e ações de regras disponíveis.

Somente a conta de administrador do Security Hub pode criar, excluir, editar e visualizar regras de automação. Uma regra criada por um administrador se aplica às descobertas na conta do administrador e nas contas dos membros. Ao fornecer IDs de contas-membro como critérios de regras, os administradores do Security Hub também podem usar regras de automação para atualizar descobertas ou agir sobre descobertas em contas-membro específicas.

> **Important**
>
> Uma regra de automação se aplica somente à Região da AWS em que foi criada. Para aplicar uma regra em várias regiões, o administrador delegado deverá criar a regra em cada região. Isso pode ser feito por meio do console do Security Hub, da API do Security Hub ou do AWS CloudFormation. Você também pode usar um script de implantação de várias regiões.

Para obter um histórico de como as regras de automação mudaram suas descobertas, consulte Analisando o histórico de descobertas.

As regras de automação se aplicam às descobertas novas e atualizadas que o Security Hub gera ou recebe após a criação da regra. O Security Hub atualiza as descobertas do controle a cada 12 a 24 horas ou quando o recurso associado muda de estado. Para obter mais informações, consulte Schedule for running security checks (Programar a execução de verificações de segurança).

Atualmente, o Security Hub oferece suporte a um máximo de 100 regras de automação para uma conta de administrador.

Ordem das regras

Ao criar regras de automação, você atribui uma ordem a cada regra. Isso determina a ordem na qual o Security Hub aplica suas regras de automação e se torna importante quando várias regras estão relacionadas à mesma descoberta ou campo de descoberta.

Quando várias ações de regra estão relacionadas à mesma descoberta ou campo de descoberta, a regra com o maior valor numérico para a ordem das regras se aplica por último e produz o efeito final.

Quando você cria uma regra no console do Security Hub, o Security Hub atribui automaticamente a ordem das regras com base na ordem de criação da regra. A regra criada mais recentemente tem o menor valor numérico para a ordem das regras e, portanto, se aplica primeiro. O Security Hub aplica regras subsequentes em ordem ascendente.

Quando você cria uma regra por meio da API Security Hub ou AWS CLI, o Security Hub aplica a regra com o menor valor numérico para a primeira `RuleOrder`. Em seguida, aplica regras subsequentes em ordem ascendente. Se várias descobertas tiverem a mesma `RuleOrder`, o Security Hub aplica uma regra com um valor anterior primeiro para o campo `UpdatedAt` (ou seja, a regra que foi editada mais recentemente se aplica por último).

É possível modificar a ordem das regras a qualquer momento.

Exemplo de ordem de regras:

Regra A (a ordem das regras é **1**):

- Critérios da Regra A
  - `ProductName` = `Security Hub`
  - `Resources.Type` é `S3 Bucket`
  - `Compliance.Status` = `FAILED`
  - `RecordState` é `NEW`

  - `Workflow.Status` = `ACTIVE`
- Ações da Regra A
  - Atualizar `Confidence` para `95`
  - Atualizar `Severity` para `CRITICAL`

Regra B (a ordem das regras é **2**):

- Critérios da Regra B
  - `AwsAccountId` = `123456789012`
- Ações de Regra B
  - Atualizar `Severity` para `INFORMATIONAL`

As ações da Regra A se aplicam primeiro às descobertas do Security Hub que correspondem aos critérios da Regra A. Em seguida, as ações da Regra B se aplicam às descobertas do Security Hub com o ID da conta especificado. Neste exemplo, como a Regra B se aplica por último, o valor final de `Severity` nas descobertas do ID da conta especificada é `INFORMATIONAL`. Com base na ação da Regra A, o valor final de `Confidence` nas descobertas correspondentes é `95`.

Critérios de regras e ações de regras disponíveis

Atualmente, os seguintes campos do ASFF são aceitos como critérios para regras de automação.

Campo do ASFF	Filtros	Tipo de campo
`AwsAccountId`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	String
`AwsAccountName`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	String
`CompanyName`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS,`	String

Campo do ASFF	Filtros	Tipo de campo
	NOT_EQUALS, PREFIX_NOT_EQUALS	
ComplianceAssociatedStandardsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ComplianceSecurityControlId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ComplianceStatus	Is, Is Not	Selecionar: [FAILED, NOT_AVAILABLE , PASSED, WARNING]
Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Número
CreatedAt	Start, End, DateRange	Data (formatada como 2022-12-01T21:47:39.269Z)
Criticality	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Número
Description	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
FirstObservedAt	Start, End, DateRange	Data (formatada como 2022-12-01T21:47:39.269Z)

Campo do ASFF	Filtros	Tipo de campo
GeneratorId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Id	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
LastObservedAt	Start, End, DateRange	Data (formatada como 2022-12-01T21:47:39.269Z)
NoteText	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
NoteUpdatedAt	Start, End, DateRange	Data (formatada como 2022-12-01T21:47:39.269Z)
NoteUpdatedBy	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ProductName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Campo do ASFF	Filtros	Tipo de campo
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Mapa
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Campo do ASFF	Filtros	Tipo de campo
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceTags	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Mapa
ResourceType	Is, Is Not	Selecione (consulte Recursos aceitos pelo ASFF)
SeverityLabel	Is, Is Not	Selecione [CRITICAL, HIGH, MEDIUM, LOW, INFORMATIONAL]
SourceUrl	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Title	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Type	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Campo do ASFF	Filtros	Tipo de campo
`UpdatedAt`	`Start, End, DateRange`	Data (formatada como 2022-12-01T21:47:39.269Z)
`UserDefinedFields`	`CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS`	Mapa
`VerificationState`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	String
`WorkflowStatus`	`Is, Is Not`	Selecionar: [`NEW`, `NOTIFIED`, `RESOLVED`, `SUPPRESSED`]

Atualmente, os seguintes campos do ASFF são aceitos como ações para regras de automação:

- `Confidence`
- `Criticality`
- `Note`
- `RelatedFindings`
- `Severity`
- `Types`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Para obter mais informações sobre campos do ASFF específicos, consulte a sintaxe do AWSFormato do Security Finding (ASFF) e exemplos de ASFF.

> **Tip**
>
> Se você quiser que o Security Hub pare de gerar descobertas para um controle específico, recomendamos desativar o controle em vez de usar uma regra de automação. Quando você desativa um controle, o Security Hub para de executar verificações de segurança nele e para de gerar descobertas para ele, para que você não incorra em cobranças por esse controle. Recomendamos o uso de regras de automação para alterar os valores de campos específicos do ASFF para descobertas que correspondam aos critérios definidos. Para obter mais informações sobre como desabilitar controles, consulte Ativando e desativando controles no padrão.

Criar regras de automação

É possível criar uma regra personalizada do zero ou usar um modelo de regra já preenchido do Security Hub.

É possível criar apenas uma regra de automação por vez. Para criar várias regras de automação, siga os procedimentos do console várias vezes ou chame a API ou o comando várias vezes com os parâmetros desejados.

Você deve criar uma regra de automação em cada região e conta na qual deseja que a regra se aplique às descobertas.

Quando você cria uma regra de automação no console do Security Hub, o Security Hub mostra uma prévia das descobertas às quais sua regra se aplica. No momento, a pré-visualização não é compatível se seus critérios de regra incluírem um filtro CONTAINS ou NOT_CONTAINS. É possível escolher esses filtros para os tipos de campo de mapa e segmento.

> **Important**
>
> A AWS recomenda não incluir informações pessoais, confidenciais ou sigilosas em seu nome de regra, descrição ou outros campos.

Criação de uma regra a partir de um modelo (somente console)

Atualmente, somente o console do Security Hub é compatível com os modelos de regras. Esses modelos refletem casos de uso comuns de regras de automação e podem ajudar você a começar a

usar o atributo. Conclua as etapas a seguir para criar uma regra de automação a partir de um modelo no console.

Console

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.

   Faça login na conta de administrador do Security Hub.
2. No painel de navegação à esquerda, escolha Automação.
3. Escolha a opção Criar regra. Em Tipo de regra, escolha Criar uma regra a partir do modelo.
4. Selecione um modelo de regra no menu suspenso.
5. (Opcional) Se necessário para seu caso de uso, modifique as seções Regra, Critérios e Ação automatizada. Especifique pelo menos um critério de regra e uma ação de regra.

   Se houver suporte para os critérios selecionados, o console mostra uma prévia das descobertas que correspondem aos seus critérios.
6. Em Status da regra, escolha se você deseja que a regra seja Habilitada ou Desabilitada depois de criada.
7. (Opcional) Expanda a seção Configurações adicionais. Selecione Ignorar regras subsequentes para descobertas que correspondam a esses critérios se quiser que essa regra seja a última regra aplicada às descobertas que correspondam aos critérios da regra.
8. (Opcional) Para Tags, adicione tags como pares de chave-valor para ajudar você a identificar facilmente a regra.
9. Escolha a opção Criar regra.

Criar uma regra personalizada

Escolha o método de sua preferência e siga as etapas a seguir para criar regras de automação personalizadas.

Console

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.

   Faça login na conta de administrador do Security Hub.
2. No painel de navegação à esquerda, escolha Automação.
3. Escolha a opção Criar regra. Em Tipo de regra, escolha Criar regra personalizada.

4. Na seção Regra, forneça um nome de regra exclusivo e uma descrição para sua regra.
5. Em Critérios, use os menus suspensos Chave, Operador e Valor para especificar seus critérios de regra. É necessário especificar pelo menos um critério de regra.

   Se houver suporte para os critérios selecionados, o console mostra uma prévia das descobertas que correspondem aos seus critérios.
6. Para Ação automatizada, use os menus suspensos para especificar quais campos de descoberta devem ser atualizados quando as descobertas corresponderem aos critérios da regra. É necessário especificar pelo menos uma ação de regra.
7. Em Status da regra, escolha se você deseja que a regra seja Habilitada ou Desabilitada depois de criada.
8. (Opcional) Expanda a seção Configurações adicionais. Selecione Ignorar regras subsequentes para descobertas que correspondam a esses critérios se quiser que essa regra seja a última regra aplicada às descobertas que correspondam aos critérios da regra.
9. (Opcional) Para Tags, adicione tags como pares de chave-valor para ajudar você a identificar facilmente a regra.
10. Escolha a opção Criar regra.

API

1. Execute o comando `CreateAutomationRule` na conta do administrador do Security Hub. Essa API cria uma regra com um nome do recurso da Amazon (ARN) específico.
2. Forneça um nome e uma descrição para a regra.
3. Defina o parâmetro `IsTerminal` como `true` se você quiser que essa regra seja a última regra aplicada às descobertas que correspondam aos critérios da regra.
4. Para o parâmetro `RuleOrder`, forneça a ordem da regra. O Security Hub aplica regras com um valor numérico menor primeiro para esse parâmetro.
5. Para o parâmetro `RuleStatus`, especifique se você deseja que o Security Hub habilite e comece a aplicar a regra às descobertas após a criação. Se nenhum valor for especificado, o padrão será `ENABLED`. Um valor `DISABLED` significa que a regra é pausada após a criação.
6. Para o parâmetro `Criteria`, forneça os critérios que você deseja que o Security Hub use para filtrar suas descobertas. A ação da regra se aplicará às descobertas que correspondam aos critérios. Para obter uma lista dos serviços compatíveis, consulte Critérios de regras e ações de regras disponíveis.

7. Para o parâmetro `Actions`, forneça as ações que você deseja que o Security Hub execute quando houver uma correspondência entre uma descoberta e seus critérios definidos. Para obter uma lista de ações compatíveis, consulte Critérios de regras e ações de regras disponíveis.

Exemplo de solicitação de API:

```
{
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
            },
            "Note": {
                "Text": "Known issue that is not a risk.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }],
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "GeneratorId": [{
            "Value": "aws-foundational-security-best-practices/v/1.0.0/IAM.1",
            "Comparison": "EQUALS"
        }]
    },
```

```
    "Description": "Sample rule description",
    "IsTerminal": false,
    "RuleName": "sample-rule-name",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
}
```

AWS CLI

1. Execute o comando `create-automation-rule` na conta do administrador do Security Hub. Esse comando cria uma regra com um nome do recurso da Amazon (ARN).
2. Forneça um nome e uma descrição para a regra.
3. Inclua o parâmetro `is-terminal` se quiser que essa regra seja a última regra aplicada às descobertas que correspondam aos critérios da regra. Caso contrário, inclua o parâmetro `no-is-terminal`.
4. Para o parâmetro `rule-order`, forneça a ordem da regra. O Security Hub aplica regras com um valor numérico menor primeiro para esse parâmetro.
5. Para o parâmetro `rule-status`, especifique se você deseja que o Security Hub habilite e comece a aplicar a regra às descobertas após a criação. Se nenhum valor for especificado, o padrão será `ENABLED`. Um valor `DISABLED` significa que a regra é pausada após a criação.
6. Para o parâmetro `criteria`, forneça os critérios que você deseja que o Security Hub use para filtrar suas descobertas. A ação da regra se aplicará às descobertas que correspondam aos critérios. Para obter uma lista dos serviços compatíveis, consulte Critérios de regras e ações de regras disponíveis.
7. Para o parâmetro `actions`, forneça as ações que você deseja que o Security Hub execute quando houver uma correspondência entre uma descoberta e seus critérios definidos. Para obter uma lista de ações compatíveis, consulte Critérios de regras e ações de regras disponíveis.

Exemplo de comando:

```
aws securityhub create-automation-rule \
--actions '[{
 "Type": "FINDING_FIELDS_UPDATE",
 "FindingFieldsUpdate": {
 "Severity": {
 "Label": "HIGH"
```

```
 },
 "Note": {
 "Text": "Known issue that is a risk. Updated by automation rules",
 "UpdatedBy": "sechub-automation"
 }
 }
 }]' \
--criteria '{
 "SeverityLabel": [{
 "Value": "INFORMATIONAL",
 "Comparison": "EQUALS"
 }]
 }' \
--description "A sample rule" \
--no-is-terminal \
--rule-name "sample rule" \
--rule-order 1 \
--rule-status "ENABLED" \
--region us-east-1
```

Visualizar regras de automação

Escolha seu método preferido e siga as etapas para visualizar suas regras de automação e os detalhes de cada regra.

Console

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.

   Faça login na conta de administrador do Security Hub.
2. No painel de navegação à esquerda, escolha Automação.
3. Escolha um nome de função. Como alternativa, selecione uma regra.
4. Escolha Ações e Visualizar.

API

1. Para visualizar as regras de automação da sua conta, execute `ListAutomationRules` a partir da conta de administrador do Security Hub. Essa API dá os ARNs da regra e outros metadados das suas regras. Nenhum parâmetro de entrada é necessário para essa API,

mas é possível fornecer opcionalmente `MaxResults` para limitar o número de resultados e `NextToken` como parâmetro de paginação. O valor inicial de `NextToken` deveria ser `NULL`.

Exemplo de solicitação de API:

```
{
 "MaxResults": 50,
 "NextToken": "cVpdnSampleTokenYcXgTockBW44c"
}
```

2. Para obter detalhes adicionais da regra, incluindo os critérios e as ações de uma regra, execute `BatchGetAutomationRules` a partir da conta de administrador do Security Hub.

   Exemplo de solicitação de API:

```
{
    "AutomationRulesArns": [
      "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
      "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
      "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
    ]
}
```

AWS CLI

1. Para visualizar as regras de automação da sua conta, execute o comando `list-automation-rules` na conta do administrador do Security Hub. Esse comando dá os ARNs da regra e outros metadados das suas regras. Nenhum parâmetro de entrada é necessário para esse comando, mas é possível fornecer opcionalmente `max-results` para limitar o número de resultados e `next-token` como parâmetro de paginação.

   Exemplo de comando:

```
aws securityhub list-automation-rules  \
--max-results 5 \
```

```
--next-token cVpdnSampleTokenYcXgTockBW44c \
--region us-east-1
```

2. Para obter detalhes adicionais da regra, incluindo os critérios e as ações de uma regra, execute o comando `batch-get-automation-rules` na conta do administrador do Security Hub.

   Exemplo de comando:

```
aws securityhub batch-get-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-
east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
 "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222"]' \
--region us-east-1
```

Editar regras de automação

Quando você edita uma regra de automação, as alterações se aplicam às descobertas novas e atualizadas que o Security Hub gera ou recebe após a edição da regra.

Escolha seu método preferido e siga as etapas para editar o conteúdo de uma regra de automação. É possível editar uma ou mais regras com uma única solicitação. Para obter instruções sobre como editar a ordem das regras, consulte Editar a ordem das regras.

Console

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.

   Faça login na conta de administrador do Security Hub.
2. No painel de navegação à esquerda, escolha Automação.
3. Selecione a regra a ser editada. Escolha Ações e Editar.
4. Altere a regra conforme desejado e escolha Salvar alterações.

API

1. Execute o comando `BatchUpdateAutomationRules` na conta do administrador do Security Hub.

2. Para o parâmetro `RuleArn`, forneça o ARN da(s) regra(s) que você deseja editar.
3. Forneça os novos valores dos parâmetros que você deseja editar. É possível editar qualquer parâmetro, exceto `RuleArn`.

Exemplo de solicitação de API:

```
{
    "UpdateAutomationRulesRequestItems": [
        {
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "RuleOrder": 15,
            "RuleStatus": "Enabled"
        },
        {
            "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
            "RuleStatus": "Disabled"
        }
    ]
}
```

AWS CLI

1. Execute o comando `batch-update-automation-rules` na conta do administrador do Security Hub.
2. Para o parâmetro `RuleArn`, forneça o ARN da(s) regra(s) que você deseja editar.
3. Forneça os novos valores dos parâmetros que você deseja editar. É possível editar qualquer parâmetro, exceto `RuleArn`.

Exemplo de comando:

```
aws securityhub batch-update-automation-rules \
--update-automation-rules-request-items '[
    {
      "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
          "Note": {
```

```
            "Text": "Known issue that is a risk",
            "UpdatedBy": "sechub-automation"
          },
          "Workflow": {
            "Status": "NEW"
          }
        }
      }],
      "Criteria": {
        "SeverityLabel": [{
         "Value": "LOW",
         "Comparison": "EQUALS"
        }]
      },
      "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "RuleOrder": 14,
      "RuleStatus": "DISABLED",
    }
  ]' \
--region us-east-1
```

Editar a ordem das regras

Em alguns casos, é possível que você queira manter os critérios e as ações da regra como estão, mas alterar a ordem na qual o Security Hub aplica uma regra de automação. Escolha seu método preferido e siga as etapas para editar a ordem das regras.

Console

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.

   Faça login na conta de administrador do Security Hub.
2. No painel de navegação à esquerda, escolha Automação.
3. Selecione a regra cuja ordem você deseja alterar. Escolha Editar prioridade.
4. Escolha Mover para cima para aumentar a prioridade da regra em uma unidade. Escolha Mover para baixo para diminuir a prioridade da regra em uma unidade. Escolha Mover para cima para atribuir à regra uma ordem de 1 (isso dá precedência a essa regra sobre outras regras existentes).

> **Note**
>
> Quando você cria uma regra no console do Security Hub, o Security Hub atribui automaticamente a ordem das regras com base na ordem de criação da regra. A regra criada mais recentemente tem o menor valor numérico para a ordem das regras e, portanto, se aplica primeiro.

API

1. Execute o comando `BatchUpdateAutomationRules` na conta do administrador do Security Hub.
2. Para o parâmetro `RuleArn`, forneça o ARN da(s) regra(s) cuja ordem você deseja editar.
3. Modifique o valor do campo `RuleOrder`.

> **Note**
>
> Se várias regras tiverem a mesma `RuleOrder`, o Security Hub aplicará uma regra com um valor anterior primeiro para o campo `UpdatedAt` (ou seja, a regra que foi editada mais recentemente se aplica por último).

AWS CLI

1. Execute o comando `batch-update-automation-rules` na conta do administrador do Security Hub.
2. Para o parâmetro `RuleArn`, forneça o ARN da(s) regra(s) cuja ordem você deseja editar.
3. Modifique o valor do campo `RuleOrder`.

> **Note**
>
> Se várias regras tiverem a mesma `RuleOrder`, o Security Hub aplicará uma regra com um valor anterior primeiro para o campo `UpdatedAt` (ou seja, a regra que foi editada mais recentemente se aplica por último).

Excluir regras de automação

Quando você exclui uma regra de automação, o Security Hub a remove da sua conta e não aplica mais a regra às descobertas.

Escolha seu método preferido e siga as etapas para excluir uma regra de automação. É possível excluir uma ou mais regras em uma única solicitação.

> **Tip**
>
> Como alternativa à exclusão, é possível desativar uma regra. Isso retém a regra para uso futuro, mas o Security Hub não aplicará a regra a nenhuma descoberta correspondente até que você a habilite.

Console

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.

   Faça login na conta de administrador do Security Hub.
2. No painel de navegação à esquerda, escolha Automação.
3. Selecione a(s) regra(s) que deseja excluir. Escolha Ação e Excluir (para reter uma regra, mas desabilite-a temporariamente e escolha Desabilitar).
4. Confirme a sua decisão e escolha Delete (Excluir).

API

1. Execute o comando `BatchDeleteAutomationRules` na conta do administrador do Security Hub.
2. Para o parâmetro `AutomationRulesArns`, forneça o ARN da(s) regra(s) que você deseja excluir (para reter uma regra, mas desabilite-a temporariamente e forneça `DISABLED` para o parâmetro `RuleStatus`).

Exemplo de solicitação de API:

```
{
    "AutomationRulesArns": [
```

```
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
        "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
    ]
}
```

AWS CLI

1. Execute o comando `batch-delete-automation-rules` na conta do administrador do Security Hub.
2. Para o parâmetro `automation-rules-arns`, forneça o ARN da(s) regra(s) que você deseja excluir (para reter uma regra, mas desabilite-a temporariamente e forneça `DISABLED` para o parâmetro `RuleStatus`).

Exemplo de comando:

```
aws securityhub batch-delete-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"]' \
--region us-east-1
```

Exemplos de regras de automação

Esta seção inclui alguns exemplos de regras de automação para casos de uso comuns. Esses exemplos correspondem aos modelos de regras no console do Security Hub.

Eleve a gravidade para Crítica quando um recurso específico, como um bucket S3, estiver em risco

Neste exemplo, os critérios da regra são combinados quando o `ResourceId` em uma descoberta é um bucket específico do Amazon Simple Storage Service (Amazon S3). A ação da regra é alterar a gravidade das descobertas correspondentes para `CRITICAL`. É possível modificar esse modelo para aplicá-lo a outros recursos.

Exemplo de solicitação de API:

```
{
    "IsTerminal": true,
    "RuleName": "Elevate severity of findings that relate to important resources",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity to CRITICAL when specific resource such as
 an S3 bucket is at risk",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "ResourceId": [{
            "Value": "arn:aws:s3:::examplebucket/developers/design_info.doc",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "This is a critical resource. Please review ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
```

```
}
```

Exemplo de comando da CLI:

```
aws securityhub create-automation-rule \
--is-terminal \
--rule-name "Elevate severity of findings that relate to important resources" \
--rule-order 1 \
--rule-status "ENABLED" \

--description "Elevate finding severity to CRITICAL when specific resource such as an
 S3 bucket is at risk" \
--criteria '{
"ProductName": [{
"Value": "Security Hub",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"ResourceId": [{
"Value": "arn:aws:s3:::examplebucket/developers/design_info.doc",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "This is a critical resource. Please review ASAP.",
```

```
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

Eleve a gravidade das descobertas relacionadas aos recursos nas contas de produção

Neste exemplo, os critérios da regra são correspondidos quando uma descoberta de gravidade `HIGH` é gerada em contas de produção específicas. A ação da regra é alterar a gravidade das descobertas correspondentes para `CRITICAL`.

Exemplo de solicitação de API:

```
{
    "IsTerminal": false,
    "RuleName": "Elevate severity for production accounts",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity from HIGH to CRITICAL for findings that
 relate to resources in specific production accounts",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "HIGH",
            "Comparison": "EQUALS"
        }],
        "AwsAccountId": [
```

```
        {
            "Value": "111122223333",
            "Comparison": "EQUALS"
        },
        {
            "Value": "123456789012",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "A resource in production accounts is at risk. Please review
 ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Exemplo de comando da CLI:

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Elevate severity of findings that relate to resources in production
 accounts" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Elevate finding severity from HIGH to CRITICAL for findings that relate
 to resources in specific production accounts" \
--criteria '{
"ProductName": [{
"Value": "Security Hub",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
```

```
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "HIGH",
"Comparison": "EQUALS"
}],
"AwsAccountId": [
{
"Value": "111122223333",
"Comparison": "EQUALS"
},
{
"Value": "123456789012",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "A resource in production accounts is at risk. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

Suprimir descobertas informativas

Neste exemplo, os critérios da regra são comparados às constatações de `INFORMATIONAL` gravidade enviadas ao Security Hub pela Amazon GuardDuty. A ação da regra é alterar o status do fluxo de trabalho das descobertas correspondentes para `SUPPRESSED`.

Exemplo de solicitação de API:

```
{
    "IsTerminal": false,
```

```
    "RuleName": "Suppress informational findings",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Suppress GuardDuty findings with INFORMATIONAL severity",
    "Criteria": {
        "ProductName": [{
            "Value": "GuardDuty",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "INFORMATIONAL",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
            },
            "Note": {
                "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL
 severity",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Exemplo de comando da CLI:

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Suppress informational findings" \
```

```
--rule-order 1 \
--rule-status "ENABLED" \
--description "Suppress GuardDuty findings with INFORMATIONAL severity" \
--criteria '{
"ProductName": [{
"Value": "GuardDuty",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "INFORMATIONAL",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Workflow": {
"Status": "SUPPRESSED"
},
"Note": {
"Text": "Automatically suppress GuardDuty findings with INFORMATIONAL severity",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

Resposta e remediação automatizadas

Com o Amazon EventBridge, é possível automatizar os serviços da AWS para responder automaticamente a eventos do sistema, como problemas de disponibilidade de aplicações ou

alterações em recursos. Os eventos dos serviços da AWS são entregues ao EventBridge quase em tempo real e de forma garantida. Você pode escrever regras simples para indicar em quais eventos você está interessado e quais ações automatizadas devem ser executadas quando um evento corresponder a uma regra. As ações que podem ser automaticamente acionadas incluem as seguintes:

- Invocar uma função do AWS Lambda
- Invocação do comando de execução do Amazon EC2
- Transmitir o evento Amazon Kinesis Data Streams
- Ativação de uma máquina de estado do AWS Step Functions
- Notificação de um tópico do Amazon SNS ou de uma fila do Amazon SQS
- Enviar uma descoberta para uma ferramenta criação de tíquetes, chat, SIEM ou gerenciamento e resposta a incidentes de terceiros

O Security Hub envia automaticamente todas as novas descobertas e todas as atualizações das descobertas existentes para o EventBridge como eventos. Você também pode criar ações personalizadas que permitem enviar descobertas selecionadas e resultados de insights para o EventBridge.

Em seguida, você configura as regras do EventBridge para responder a cada tipo de evento.

Para obter mais informações sobre como usar o EventBridge, consulte o Guia do usuário do Amazon EventBridge.

> **Note**
>
> Como prática recomendada, certifique-se de que as permissões concedidas aos usuários para acessar o EventBridge usem políticas do IAM com privilégios mínimos que concedam apenas as permissões necessárias.
> Para obter mais informações, consulte Gerenciamento de identidade e acesso no Amazon EventBridge..

Um conjunto de modelos para resposta e remediação automatizadas entre contas também está disponível em Soluções AWS. Os modelos utilizam as regras de eventos do EventBridge e as funções do Lambda. Você implanta a solução usando AWS CloudFormation e AWS Systems Manager. A solução pode criar ações de resposta e remediação totalmente automatizadas. Ela

também pode usar ações personalizadas do Security Hub para criar ações de resposta e remediação acionadas pelo usuário. Para obter detalhes sobre como configurar e usar a solução, consulte a página Resposta de segurança automatizada em AWS.

Tópicos

Tipos de integração do Security Hub com o EventBridge

O Security Hub usa os seguintes tipos de eventos do EventBridge para oferecer suporte aos seguintes tipos de integração com o EventBridge.

No painel do EventBridge para Security Hub, Todos os eventos inclui todos esses tipos de eventos.

Todas as descobertas (Security Hub Findings - Imported)

O Security Hub envia automaticamente todas as novas descobertas e todas as atualizações das descobertas existentes para o EventBridge como eventos Security Hub Findings - Imported. Cada evento Security Hub Findings - Importedcontém uma única descoberta.

Cada solicitação `BatchImportFindings` e `BatchUpdateFindings` aciona um evento Security Hub Findings - Imported.

Para contas de administrador, o feed de eventos no EventBridge inclui eventos para descobertas de suas contas e de suas contas de membros.

Em uma região de agregação, o feed de eventos inclui eventos para descobertas da região de agregação e das regiões vinculadas. As descobertas entre regiões são incluídas no feed de eventos quase em tempo real. Para obter informações sobre como configurar a agregação de descoberta, consulte Agregação entre regiões.

Você pode definir regras no EventBridge que roteiam automaticamente as descobertas para um bucket do Amazon S3, um fluxo de trabalho de correção ou uma ferramenta de terceiros. As regras podem incluir filtros que só aplicam a regra se a descoberta tiver valores de atributos específicos.

Você usa esse método para enviar automaticamente todas as descobertas, ou todas as descobertas que possuem características específicas, para um fluxo de trabalho de resposta ou correção.

Consulte the section called “Configurar uma regra para enviar descobertas automaticamente ”.

Descobertas para ações personalizadas (Security Hub Findings - Custom Action)

O Security Hub também envia descobertas associadas a ações personalizadas para o EventBridge como eventos Security Hub Findings - Custom Action .

Isso é útil para analistas que trabalham com o console do Security Hub e desejam enviar uma descoberta específica, ou um pequeno conjunto de descobertas, para um fluxo de trabalho de resposta ou correção. É possível selecionar uma ação personalizada para até 20 descobertas por vez. Cada descoberta é enviada para o EventBridge como um evento separado do EventBridge.

Ao criar uma ação personalizada, você atribui a ela uma ID de ação personalizada. Você pode usar essa ID para criar uma regra do EventBridge que executa uma ação específica após receber uma descoberta associada a essa ID de ação personalizada.

Consulte the section called “Configurando e usando ações personalizadas”.

Por exemplo, você pode criar uma ação personalizada no Security Hub chamada `send_to_ticketing`. Em seguida, no EventBridge, você cria uma regra que é acionada quando o EventBridge recebe uma descoberta que inclui o `send_to_ticketing` do ID da ação personalizada. A regra inclui a lógica para enviar a descoberta ao sistema de emissão de tíquetes. Você pode então selecionar descobertas no Security Hub e usar a ação personalizada nele para enviar manualmente as descobertas ao seu sistema de tickets.

Para obter exemplos de como enviar descobertas do Security Hub ao EventBridge para processamento adicional, consulte Como integrar AWS Security Hub ações personalizadas ao PagerDuty e Como habilitar ações personalizadas no AWS Security Hub no blog AWS Partner Network (APN).

Resultados de insight para ações personalizadas (Security Hub Insight Results)

Você também pode usar ações personalizadas para enviar conjuntos de resultados de insights ao EventBridge como eventos Security Hub Insight Results. Os resultados do insight são os recursos que combinam com um insight. Observe que ao enviar resultados de insights para o EventBridge, você não está enviando as descobertas para o EventBridge. Você está enviando

apenas os identificadores de recursos associados aos resultados do insight. É possível enviar até 100 identificadores de recursos de uma vez.

Semelhante às ações personalizadas para descobertas, primeiro você cria a ação personalizada no Security Hub e, em seguida, cria uma regra no EventBridge.

Consulte the section called “Configurando e usando ações personalizadas”.

Por exemplo, suponha que você veja um resultado interessante de um insight específico que deseja compartilhar com um colega. Nesse caso, você pode usar uma ação personalizada para enviar o resultado do insight para o colega por meio de um sistema de bate-papo ou emissão de tíquetes.

Formatos de eventos do EventBridge para o Security Hub

Os tipos de eventos Security Hub Findings - Imported, Security Findings - Custom Action, e Security Hub Insight Results usam os formatos de evento a seguir.

O formato do evento é aquele usado quando o Security Hub envia um evento para o EventBridge.

Security Hub Findings - Imported

Security Hub Findings - Imported os eventos enviados do Security Hub para o EventBridge usam o seguinte formato.

```
{
   "version":"0",
   "id":"CWE-event-id",
   "detail-type":"Security Hub Findings - Imported",
   "source":"aws.securityhub",
   "account":"111122223333",
   "time":"2019-04-11T21:52:17Z",
   "region":"us-west-2",
   "resources":[
      "arn:aws:securityhub:us-west-2::product/aws/macie/arn:aws:macie:us-
west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/
f2893b211841"
   ],
   "detail":{
      "findings": [{
         <finding content>
       }]
   }
```

```
}
```

<finding content> é o conteúdo, no formato JSON, da descoberta enviada pelo evento. Cada evento envia uma única descoberta.

Para obter uma lista completa de atributos de descoberta, consulte AWS Formato de descoberta de segurança (ASFF).

Para obter informações sobre como configurar as regras do EventBridge que são acionadas por esses eventos, consulte the section called “Configurar uma regra para enviar descobertas automaticamente ”.

Security Hub Findings - Custom Action

Security Hub Findings - Custom Action os eventos enviados do Security Hub para o EventBridge usam o seguinte formato. Cada descoberta é enviada em um evento separado.

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Findings - Custom Action",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2019-04-11T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:securityhub:us-west-1:111122223333:action/custom/custom-action-name"
  ],
  "detail": {
    "actionName":"custom-action-name",
    "actionDescription": "description of the action",
    "findings": [
      {
        <finding content>
      }
    ]
  }
}
```

<finding content> é o conteúdo, no formato JSON, da descoberta enviada pelo evento. Cada evento envia uma única descoberta.

Para obter uma lista completa de atributos de descoberta, consulte AWS Formato de descoberta de segurança (ASFF).

Para obter informações sobre como configurar as regras do EventBridge que são acionadas por esses eventos, consulte the section called “Configurando e usando ações personalizadas”.

Security Hub Insight Results

Security Hub Insight Results os eventos enviados do Security Hub para o EventBridge usam o seguinte formato.

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Insight Results",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": [
      "arn:aws:securityhub:us-west-1:111122223333::product/aws/macie:us-
west-1:222233334444:test/trigger/1ec9cf700ef6be062b19584e0b7d84ec/alert/f2893b211841"
  ],
  "detail": {
    "actionName":"name of the action",
    "actionDescription":"description of the action",
    "insightArn":"ARN of the insight",
    "insightName":"Name of the insight",
    "resultType":"ResourceAwsIamAccessKeyUserName",
    "number of results":"number of results, max of 100",
    "insightResults": [
        {"result 1": 5},
        {"result 2": 6}
    ]
  }
}
```

Para obter informações sobre como criar uma regra do EventBridge que seja acionada por esses eventos, consulte the section called “Configurando e usando ações personalizadas”.

Configurar uma regra do EventBridge para enviar descobertas automaticamente

Você pode criar uma regra no EventBridge que define uma ação a ser tomada quando um evento do Security Hub Findings - Imported é recebido. Os eventos doSecurity Hub Findings - Imported são acionados por atualizações de `BatchImportFindings` e `BatchUpdateFindings`.

Cada regra contém um padrão de evento, que identifica os eventos que acionam a regra. O padrão do evento sempre contém a fonte do evento (`aws.securityhub`) e o tipo de evento (Security Hub Findings - Imported). O padrão do evento também pode especificar filtros para identificar as descobertas às quais a regra se aplica.

A regra então identifica os alvos da regra. Os alvos são as ações a serem tomadas quando o EventBridge recebe um evento Security Hub Findings - Imported e a descoberta corresponde aos filtros.

As instruções fornecidas aqui usam o console do EventBridge. Quando você usa o console, o EventBridge cria automaticamente a política baseada em recursos necessária que permite que o EventBridge grave para o CloudWatch logs.

Você também pode usar a operação `PutRule` da API da EventBridge. No entanto, se você usar a API do EventBridge, deverá criar a política baseada em recursos. Para obter detalhes sobre a política necessária, consulte as permissões do CloudWatch Logs no Guia do usuário do Amazon EventBridge.

Formato do padrão do evento

O formato do padrão de eventos para os eventos Security Hub Findings - Imported é o seguinte:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
```

```
}
```

- `source` identifica o Security Hub como o serviço que gera o evento.
- `detail-type` identifica o tipo de evento.
- `detail` é opcional e fornece os valores do filtro para o padrão do evento. Se o padrão do evento não contiver um campo `detail`, todas as descobertas acionarão a regra.

Você pode filtrar as descobertas com base em qualquer atributo de descoberta. Para cada atributo, você fornece uma matriz separada por vírgula de um ou mais valores.

```
"<attribute name>": [ "<value1>", "<value2>"]
```

Se você fornecer mais de um valor para um atributo, esses valores serão unidos por `OR`. Uma descoberta corresponde ao filtro de um atributo individual se a descoberta tiver algum dos valores listados. Por exemplo, se você fornecer ambos `INFORMATIONAL` e `LOW` como valores para `Severity.Label`, a descoberta corresponderá se tiver um rótulo de severidade de `INFORMATIONAL` ou`LOW`.

Os atributos são unidos por `AND`. Uma descoberta corresponde se atender aos critérios de filtro de todos os atributos fornecidos.

Quando você fornece um valor de atributo, ele deve refletir a localização desse atributo na estrutura do AWS Formato do Security Finding (ASFF).

> **Tip**
>
> Ao filtrar as descobertas do controle, recomendamos usar os campos do ASFF `SecurityControlId` ou `SecurityControlArn` como filtros, em vez de `Title` ou `Description`. Os últimos campos podem mudar ocasionalmente, enquanto o ID de controle e o ARN são identificadores estáticos.

No exemplo a seguir, o padrão de evento fornece valores de filtro para `ProductArn` e`Severity.Label`, portanto, uma descoberta corresponde se for gerada pelo Amazon Inspector e tiver um rótulo de severidade de`INFORMATIONAL` ou `LOW`.

```
{
```

```
    "source": [
        "aws.securityhub"
     ],
    "detail-type": [
        "Security Hub Findings - Imported"
    ],
    "detail": {
        "findings": {
            "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
            "Severity": {
                "Label": ["INFORMATIONAL", "LOW"]
            }
        }
    }
}
```

Criar uma regra de evento

Você pode usar um padrão de evento predefinido ou um padrão de evento personalizado para criar uma regra no EventBridge. Se você selecionar um padrão predefinido, o EventBridge preencherá automaticamente em `source` e `detail-type`. O EventBridge também fornece campos para especificar valores de filtro para os seguintes atributos de descoberta:

- `AwsAccountId`
- `Compliance.Status`
- `Criticality`
- `ProductArn`
- `RecordState`
- `ResourceId`
- `ResourceType`
- `Severity.Label`
- `Types`
- `Workflow.Status`

Para criar uma regra de EventBridge

1. Abra o console Amazon EventBridge em https://console.aws.amazon.com/events/.

2. Usando os valores a seguir, crie uma regra no EventBridge que monitore os eventos de descoberta:

   - Em Tipo de regra, escolha Regra com um padrão de evento.
   - Selecione como criar o padrão do evento.

Para criar o padrão de eventos com...	Fazer isso...
Um modelo	Na seção Padrão de evento, selecione um dos seguintes procedimentos: • Em Event source (Origem do evento), selecione AWS services (Serviços da). • Em AWS serviço, escolha Security Hub. • Em Tipo de evento, selecione Security Hub Findings - Imported. • (Opcional) Para tornar a regra mais específica, adicione valores de filtros. Por exemplo, para limitar a regra às descobertas com estados de registro ativos, em Estado(s) de registro específico, selecione Ativo.

Para criar o padrão de eventos com...	Fazer isso...
Um padrão de eventos personalizado (Use um padrão personalizado se quiser filtrar as descobertas com base em atributos que não aparecem no console do EventBridge.)	• Em Padrão de evento, selecione JSON editor, e, em seguida, cole um dos seguintes exemplos de padrão de evento na área de texto: `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "<attribute name>": [ "<value1>", "<value2>" ] } } }` • Atualize o padrão do evento para incluir o atributo e os valores de atributos que você deseja usar como filtro. Por exemplo, para aplicar a regra às descobertas que têm um estado de verificação de

Para criar o padrão de eventos com...	Fazer isso...	
	`TRUE_POSITIVE` , use o seguinte exemplo de padrão: `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "VerificationState": ["TRUE_POSITIVE"] } } }`	

- Em Tipos de destino, escolha Serviço da AWS, e em Selecionar um destino, escolha um destino, como um tópico do Amazon SNS ou uma função do AWS Lambda. O destino é acionado quando é recebido um evento que corresponde ao padrão de evento definido na regra.

Para saber mais sobre a criação de regras, consulte Criar regras do Amazon EventBridge que reajam a eventos no Guia do usuário do Amazon EventBridge.

Usando ações personalizadas para enviar descobertas e resultados de insights para o EventBridge

Para usar as ações personalizadas do Security Hub para enviar descobertas ou resultados de insights para o EventBridge, primeiro crie a ação personalizada no Security Hub. Em seguida, defina regras no EventBridge que se apliquem às suas ações personalizadas.

É possível criar até 50 ações personalizadas.

Se você habilitou a agregação entre regiões e gerenciou as descobertas da região de agregação, crie ações personalizadas na região de agregação.

A regra no EventBridge usa o ARN da ação personalizada.

Criar uma ação personalizada (console)

Ao criar uma ação personalizada, especifique o nome, a descrição e um identificador exclusivo.

Para criar uma ação personalizada no Security Hub (console)

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Settings (Configurações) e Custom actions (Ações personalizadas).
3. Escolha Create custom action (Criar ação personalizada).
4. Forneça um Name (Nome), uma Description (Descrição) e um Custom action ID (ID da ação personalizada) à ação.

   O Name (Nome) deve ter menos de 20 caracteres.

   O Custom action ID deve ser exclusivo para cada conta da AWS.
5. Escolha Create custom action (Criar ação personalizada).
6. Anote o Custom action ARN (ARN da ação personalizada). É necessário usar o ARN ao criar uma regra para associar a essa ação no EventBridge.

Criação de uma ação personalizada (API do Security Hub, AWS CLI)

Para criar uma ação personalizada, você pode usar uma chamada de API ou o AWS Command Line Interface.

Para criar uma ação personalizada (API do Security Hub, AWS CLI)

- API do Security Hub – use a operação API `CreateActionTarget`. Ao criar uma ação personalizada, você fornece o nome, a descrição e o identificador da ação personalizada.
- AWS CLI – na linha de comando, execute o comando `create-action-target`.

```
create-action-target --name <customActionName> --
description <customActionDescription> --id <customActionidentifier>
```

Exemplo

```
aws securityhub create-action-target --name "Send to remediation" --description
 "Action to send the finding for remediation tracking" --id "Remediation"
```

Definindo uma regra no EventBridge

Para processar a ação personalizada, você deve criar uma regra correspondente no EventBridge. A definição da regra inclui o ARN da ação personalizada.

O padrão de evento para um evento Security Hub Findings - Custom Action tem o seguinte formato:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

O padrão de evento para um evento Security Hub Insight Results tem o seguinte formato:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
```

```
  "resources": [ "<custom action ARN>" ]
}
```

Em ambos os padrões, *<custom action ARN>* é o ARN de uma ação personalizada. Você pode configurar uma regra que se aplique a mais de uma ação personalizada.

As instruções fornecidas aqui são para o console do EventBridge. Quando você usa o console, o EventBridge cria automaticamente a política baseada em recursos necessária que permite que o EventBridge grave para o CloudWatch logs.

Você também pode usar a operação `PutRule` da API da EventBridge. No entanto, se você usar a API do EventBridge, deverá criar a política baseada em recursos. Para obter detalhes sobre a política necessária, consulte as permissões do CloudWatch Logs no Guia do usuário do Amazon EventBridge.

Para definir uma regra no EventBridge

1. Abra o console Amazon EventBridge em https://console.aws.amazon.com/events/.
2. No painel de navegação, escolha Regras.
3. Selecione Criar regra.
4. Insira um nome e uma descrição para a regra.
5. Em Event bus, escolha o barramento de eventos que você deseja associar a essa regra. Se quiser que essa regra faça a correspondência com eventos provenientes da sua conta, selecione padrão. Quando um serviço da AWS em sua conta emite um evento, ele sempre vai para o barramento de eventos padrão da sua conta.
6. Em Rule type (Tipo de regra), selecione Rule with an event pattern (Regra com um padrão de evento).
7. Escolha Next (Próximo).
8. Em Origem de eventos, escolha Eventos da AWS.
9. Na seção Padrão de eventos, selecione Formulário de padrão de eventos.
10. Em Event source (Origem do evento), selecione AWS services (Serviços da).
11. Para o AWSserviço, selecione Security Hub.
12. Em Event type (Tipo de evento), siga um destes procedimentos:

    - Para criar uma regra a ser aplicada ao enviar descobertas para uma ação personalizada, selecione Security Hub Findings - Custom Action.

- Para criar uma regra a ser aplicada ao enviar os resultados do insight para uma ação personalizada, selecione Security Hub Insight Results.

13. Selecione ARNs de ações personalizadas específicas e adicione um ARN de ação personalizada.

    Se a regra se aplicar a várias ações personalizadas, selecione Adicionar para adicionar mais ARNs de ações personalizadas.
14. Escolha Next (Próximo).
15. Em Adicionar destino, selecione e configure destino a ser invocado quando essa regra for correspondida.
16. Escolha Next (Próximo).
17. (Opcional) Insira uma ou mais tags para a regra. Para mais informações, consulte Tags Amazon EventBridge em Guia de Usuário Amazon EventBridge.
18. Escolha Next (Próximo).
19. Analise os detalhes da regra e selecione Criar regra.

    Quando você executa uma ação personalizada em descobertas ou resultados de insights em sua conta, são gerados eventos no EventBridge.

Seleção de uma ação personalizada para descobertas e resultados de insights

Depois que você criar suas ações personalizadas do SecurityHub e as regras do EventBridge, você poderá enviar descobertas e resultados de insights ao EventBright para obter gerenciamento e processamento adicionais.

Os eventos são enviados ao EventBridge somente na conta em que são visualizados. Se você visualizar uma descoberta usando uma conta de administrador, o evento será enviado para a EventBridge na conta do administrador.

Para que as chamadas de API da AWS sejam eficazes, as implementações do código de destino devem mudar de função para contas de membro. Isso também significa que a função para a qual você muda deve ser distribuída a cada membro onde uma ação for necessária.

Para enviar descobertas para a EventBridge

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.
2. Exiba uma lista das descobertas:

- Em Descobertas, você pode visualizar as descobertas de todas as integrações e controles de produtos habilitados.
- Em Padrões de segurança, você pode navegar até uma lista de descobertas geradas a partir de um controle selecionado. Consulte the section called “Visualizar detalhes de controles”.
- Em Integrações, você pode navegar até uma lista de descobertas geradas por uma integração habilitada. Consulte the section called “Visualizar as descobertas de uma integração”.
- Em Insights, você pode navegar até uma lista de descobertas para um resultado de insight. Consulte the section called “Visualizar resultados e descobertas de insight”.

3. Selecione as descobertas para enviar ao EventBridge É possível selecionar até 20 descobertas por vez.
4. Em Ações, selecione a ação personalizada que se alinha à regra do EventBridge a ser aplicada.

   O Security Hub envia um evento separado Security Hub Findings - Custom Action para cada descoberta.

Para enviar resultados de insights para o EventBridge

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Insights.
3. Na página Insights, selecione o insight que inclui os resultados para enviar ao EventBridge.
4. Selecione os resultados do insight a serem enviados ao EventBridge. Você pode selecionar até 20 descobertas por vez.
5. Em Ações, selecione a ação personalizada que se alinha à regra do EventBridge a ser aplicada.

Integrações de produtos no AWS Security Hub

O AWS Security Hub pode agregar dados de descoberta de segurança de diversos serviços da AWS e de soluções de segurança compatíveis da Rede de parceiros da AWS (APN). Essa agregação fornece uma visão abrangente de segurança e conformidade em todo o seu ambiente AWS.

Também é possível enviar descobertas que são geradas de seus próprios produtos de segurança personalizados.

> **Important**
>
> A partir das integrações de produtos da AWS e de parceiros com suporte, o Security Hub recebe e consolida apenas as descobertas geradas depois que você habilita o Security Hub em seu Contas da AWS.
> O serviço não recebe e consolida retroativamente as descobertas de segurança geradas antes de você ativar o Security Hub.

Para obter detalhes sobre como o Security Hub cobra pelas descobertas ingeridas, consulte preços do Security Hub.

Tópicos

Gerenciar integrações de produtos

A página Integrações no AWS Management Console fornece acesso a todas as integrações de produtos disponíveis AWS e de terceiros. A API do AWS Security Hub também fornece operações para permitir que você gerencie integrações.

> **Note**
>
> Algumas integrações não estão disponíveis em todas as regiões Se uma integração não for compatível na região atual, ela não será listada na página Integrações.

Consulte também the section called “Integrações com suporte na China (Pequim) e na China (Ningxia)” e the section called “Integrações que são suportadas em AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA)”.

Visualizar e filtrar a lista de integrações (console)

Na página Integrações, é possível visualizar e filtrar a lista de integrações.

Como exibir a lista de integrações

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação do Security Hub, selecione Integrações.

Na página Integrações, as integrações com outros serviços da AWS são listadas primeiro, seguidas pelas integrações com produtos de terceiros.

Para cada integração, a página Integrações fornece as seguintes informações.

- O nome da empresa
- O nome do produto
- Uma descrição da integração
- As categorias às quais a integração se aplica
- Como habilitar a integração
- O status atual da integração

Você pode filtrar a lista inserindo o texto dos seguintes campos.

- Company name (Nome da empresa)
- Nome do produto
- Descrição da integração
- Categorias

Visualizando informações sobre integrações de produtos (API do Security Hub) AWS CLI

Para ver informações sobre integrações de produtos, você pode usar uma chamada de API ou o AWS Command Line Interface. Você pode exibir informações sobre todas as integrações de produtos ou informações sobre as integrações de produtos que você habilitou.

Para ver informações sobre todas as integrações de produtos disponíveis (API Security Hub, AWS CLI)

- API Security Hub: use a operação `DescribeProducts`. Para identificar uma integração de produto específica a ser retornada, use o parâmetro `ProductArn` para fornecer o ARN de integração.
- AWS CLI: na linha de comando, execute o comando `describe-products`. Para identificar uma integração de produto específica a retornar, forneça o ARN de integração.

```
aws securityhub describe-products --product-arn "<integrationARN>"
```

Exemplo

```
aws securityhub describe-products --product-arn "arn:aws:securityhub:us-
east-1::product/3coresec/3coresec"
```

Para visualizar informações sobre as integrações de produtos que você habilitou (API Security Hub, AWS CLI)

- API do Security Hub – use a operação API `ListEnabledProductsForImport`.
- AWS CLI: na linha de comando, execute o comando `list-enabled-products-for-import`.

```
aws securityhub list-enabled-products-for-import
```

Habilitar uma integração

Na página Integrações, cada integração fornece as etapas necessárias para habilitar a integração.

Para a maioria das integrações com outros AWS serviços, a única etapa necessária é habilitar o outro serviço. As informações de integração incluem um link para a página inicial do serviço. Quando você habilita o outro serviço, uma permissão de recurso que permite que o Security Hub receba descobertas do serviço é automaticamente criada e aplicada.

Para integrações de produtos de terceiros, talvez seja necessário comprar a integração no e AWS Marketplace, em seguida, configurar a integração. As informações de integração fornecem links para realizar essas tarefas.

Se mais de uma versão de um produto estiver disponível AWS Marketplace, selecione a versão para assinar e escolha Continuar para assinar. Por exemplo, alguns produtos oferecem uma versão padrão e uma AWS GovCloud (US) versão.

Quando você ativa uma integração de produtos, uma política de recursos é anexada automaticamente à assinatura desse produto. Essa política de recursos define as permissões necessárias para o Security Hub receber as descobertas desse produto.

Desabilitar e habilitar o fluxo de descobertas em uma integração (console)

Na página Integrações, para integrações que enviam descobertas, a informação de Status indica se você está aceitando descobertas no momento.

Para parar de aceitar descobertas, escolha Stop accepting findings (Parar de aceitar descobertas).

Para continuar aceitando descobertas, escolha Accept findings (Aceitar descobertas).

Desabilitando o fluxo de descobertas de uma integração (API do Security Hub) AWS CLI

Para desativar o fluxo de descobertas em uma integração, você pode usar uma chamada de API ou o AWS Command Line Interface.

Para desativar o fluxo de descobertas de uma integração (API do Security Hub AWS CLI)

- API do Security Hub – use a operação API `DisableImportFindingsForProduct`. Para identificar a integração a ser desabilitada, você precisa do ARN da sua assinatura. Para obter os ARNs de assinatura para as integrações habilitadas, use a operação `ListEnabledProductsForImport`.
- AWS CLI: na linha de comando, execute o comando `disable-import-findings-for-product`.

```
aws securityhub disable-import-findings-for-product --product-subscription-
arn <subscription ARN>
```

Exemplo

```
aws securityhub disable-import-findings-for-product --product-subscription-arn
 "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/
crowdstrike-falcon"
```

Habilitando o fluxo de descobertas a partir de uma integração (API do Security Hub AWS CLI)

Para habilitar o fluxo de descobertas de uma integração, você pode usar uma chamada de API ou o AWS Command Line Interface.

Para permitir o fluxo de descobertas de uma integração (API do Security Hub AWS CLI)

- API do Security Hub – use a operação API `EnableImportFindingsForProduct`. Para habilitar que o Security Hub receba descobertas de uma integração, você precisa do ARN do produto. Para obter os ARNs das integrações disponíveis, use a operação `DescribeProducts`.
- AWS CLI: na linha de comando, execute o comando `enable-import-findings-for-product`.

```
aws securityhub enable-import-findings-for-product --product-arn <integration ARN>
```

Exemplo

```
aws securityhub enable-import-findings-for product --product-arn
 "arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

Visualizar as descobertas de uma integração

Para integrações para as quais você está aceitando descobertas (Status é Aceitar descobertas), para visualizar uma lista de descobertas, escolha Ver descobertas.

A lista de descobertas mostra as descobertas ativas para a integração selecionada que têm um status de fluxo de trabalho de `NEW` ou `NOTIFIED`.

Se você habilitar a agregação entre regiões, na região de agregação, a lista incluirá descobertas da região de agregação e de regiões vinculadas nas quais a integração está habilitada. O Security Hub não habilita automaticamente as integrações com base na configuração de agregação entre regiões.

Em outras regiões, a lista de descobertas de uma integração contém somente descobertas da região atual.

Para obter informações sobre como configurar a agregação entre regiões, consulte. Agregação entre regiões

Na lista de descobertas, é possível executar as ações a seguir.

- Alterar os filtros e o agrupamento da lista
- Visualizar detalhes de descobertas individuais
- Atualizar o status do fluxo de trabalho das descobertas
- Enviar descobertas para ações personalizadas

AWS service (Serviço da AWS) integrações com o AWS Security Hub

AWS O Security Hub oferece suporte a integrações com vários outros Serviços da AWS.

> **Note**
>
> Algumas integrações só estão disponíveis em select Regiões da AWS.
> Se uma integração não for compatível em uma região específica, ela não estará listada na página Integrações do console do Security Hub.
> Para obter mais informações, consulte Integrações com suporte na China (Pequim) e na China (Ningxia) e Integrações que são suportadas em AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA).

A menos que indicado abaixo, AWS service (Serviço da AWS) as integrações que enviam descobertas para o Security Hub são ativadas automaticamente após a ativação do Security Hub.

As integrações que recebem as descobertas do Security Hub podem exigir etapas adicionais para ativação. Analise as informações sobre cada integração para saber mais.

Visão geral das integrações AWS de serviços com o Security Hub

Aqui está uma visão geral dos AWS serviços que enviam descobertas para o Security Hub ou recebem descobertas do Security Hub.

AWS Serviço integrado	Direction
AWS Config	Envia descobertas
AWS Firewall Manager	Envia descobertas
Amazon GuardDuty	Envia descobertas
AWS Health	Envia descobertas
AWS Identity and Access Management Access Analyzer	Envia descobertas
Amazon Inspector	Envia descobertas
AWS IoT Device Defender	Envia descobertas
Amazon Macie	Envia descobertas
AWS Systems Manager Patch Manager	Envia descobertas
AWS Audit Manager	Recebe descobertas
AWS Chatbot	Recebe descobertas
Amazon Detective	Recebe descobertas
Amazon Security Lake	Recebe descobertas
AWS Systems Manager Explorer e OpsCenter	Recebe e atualiza as descobertas

AWS Serviço integrado	Direction	
AWS Trusted Advisor	Recebe descobertas	

AWS serviços que enviam descobertas para o Security Hub

Os AWS serviços a seguir se integram ao Security Hub enviando descobertas para o Security Hub. O Security Hub transforma as descobertas para o AWS Formato do Security Finding.

AWS Config (Envia descobertas)

AWS Config é um serviço que permite avaliar, auditar e avaliar as configurações de seus AWS recursos. AWS Config monitora e registra continuamente suas configurações de AWS recursos e permite automatizar a avaliação das configurações gravadas em relação às configurações desejadas.

Ao usar a integração com AWS Config, você pode ver os resultados das avaliações de regras AWS Config gerenciadas e personalizadas como descobertas no Security Hub. Essas descobertas podem ser visualizadas com outras descobertas do Security Hub, fornecendo uma visão geral abrangente de sua postura de segurança.

AWS Config usa EventBridge a Amazon para enviar avaliações de AWS Config regras ao Security Hub. O Security Hub transforma as avaliações de regras em descobertas que seguem o Formato do Security Finding AWS. Em seguida, o Security Hub enriquece as descobertas com base no melhor esforço, obtendo mais informações sobre os recursos afetados, como o nome do recurso da Amazon (ARN) e a data de criação. As tags de recursos nas avaliações de AWS Config regras não estão incluídas nas descobertas do Security Hub.

Para mais informações sobre esta integração, consulte as seções a seguir.

Como AWS Config envia descobertas para o Security Hub

Todas as descobertas no Security Hub usam o formato padrão JSON do ASFF. O ASFF inclui detalhes sobre a origem da descoberta, o recurso afetado e o status atual da descoberta. AWS Config envia avaliações de regras gerenciadas e personalizadas para o Security Hub via EventBridge. O Security Hub transforma as avaliações de regras em descobertas que seguem o ASFF e enriquece as descobertas com base no melhor esforço.

Tipos de descobertas que são AWS Config enviadas ao Security Hub

Depois que a integração é ativada, AWS Config envia avaliações de todas as regras AWS Config gerenciadas e personalizadas para o Security Hub. Somente avaliações de AWS Config regras vinculadas a serviços, como aquelas usadas para executar verificações nos controles de segurança, são excluídas.

Enviando AWS Config descobertas para o Security Hub

Quando a integração for ativada, o Security Hub atribuirá automaticamente as permissões necessárias para receber as descobertas AWS Config. O Security Hub usa permissões de service-to-service nível que fornecem uma maneira segura de ativar essa integração e importar descobertas AWS Config via Amazon EventBridge.

Latência para enviar descobertas

Quando AWS Config cria uma nova descoberta, geralmente você pode visualizá-la no Security Hub em cinco minutos.

Tentar novamente quando o Security Hub não estiver disponível

AWS Config envia as descobertas para o Security Hub com base no melhor esforço, por meio de EventBridge. Quando um evento não é entregue com sucesso ao Security Hub, EventBridge repita a entrega por até 24 horas ou 185 vezes, o que ocorrer primeiro.

Atualizando as AWS Config descobertas existentes no Security Hub

Depois de AWS Config enviar uma descoberta para o Security Hub, ele pode enviar atualizações da mesma descoberta para o Security Hub para refletir observações adicionais da atividade de descoberta. As atualizações são enviadas somente para eventos `ComplianceChangeNotification`. Se nenhuma alteração de conformidade ocorrer, as atualizações não serão enviadas para o Security Hub. O Security Hub exclui as descobertas 90 dias após a atualização mais recente ou 90 dias após a criação, se nenhuma atualização ocorrer.

O Security Hub não arquiva as descobertas enviadas, AWS Config mesmo que você exclua o recurso associado.

Regiões nas quais existem AWS Config descobertas

AWS Config as descobertas ocorrem em uma base regional. AWS Config envia as descobertas para o Security Hub na mesma região ou regiões em que as descobertas ocorrem.

Visualizando AWS Config descobertas no Security Hub

Para ver suas AWS Config descobertas, escolha Descobertas no painel de navegação do Security Hub. Para filtrar as descobertas para exibir somente AWS Config as descobertas, escolha Nome do produto no menu suspenso da barra de pesquisa. Insira Config e escolha Aplicar.

Interpretando AWS Config encontrar nomes no Security Hub

O Security Hub transforma avaliações de AWS Config regras em descobertas que seguem o. AWS Formato de descoberta de segurança (ASFF) AWS Config as avaliações de regras usam um padrão de eventos diferente em comparação com o ASFF. A tabela a seguir mapeia os campos de avaliação da AWS Config regra com seus equivalentes do ASFF conforme eles aparecem no Security Hub.

Tipo de descoberta da avaliação da regra de configuração	Tipo de descoberta do ASFF	Valor codificado
detalhe. awsAccountId	AwsAccountId	
detalhe. newEvaluationResult. resultRecordedTime	CreatedAt	
detalhe. newEvaluationResult. resultRecordedTime	UpdatedAt	
	ProductArn	"arn:<partition>:securityhub:<region>::product/aws/config"
	ProductName	“Config”
	CompanyName	"AWS"
	Região	“eu-central-1”
configRuleArn	GeneratorId, ProductFields	
detalhe. ConfigRuleARN/Descoberta/Hash	Id	

Tipo de descoberta da avaliação da regra de configuração	Tipo de descoberta do ASFF	Valor codificado
detalhe. configRuleName	Título, ProductFields	
detalhe. configRuleName	Descrição	“Essa descoberta foi criada para uma alteração de conformidade de recurso para a regra de configuração: `${detail.ConfigRuleName}` ”
Item de configuração “ARN” ou ARN computado do Security Hub	Resources[i].id	
detail.resourceType	Resources[i].Type	"AwsS3Bucket"
	Resources[i].Partition	"aws"
	Resources[i].Region	“eu-central-1”
Item de configuração “configuração”	Resources[i].Details	
	SchemaVersion	"2018-10-08"
	Severity.Label	Consulte “Interpretar o rótulo de gravidade” abaixo
	Tipos	[“Verificações de Software e Configuração”]
detalhe. newEvaluationResult. Tipo de conformidade	Compliance.Status	"REPROVADO", "NÃO_DISPONÍVEL", "APROVADO", ou "AVISO"

Tipo de descoberta da avaliação da regra de configuração	Tipo de descoberta do ASFF	Valor codificado
	Workflow.Status	“RESOLVIDO” se uma AWS Config descoberta for gerada com um status de conformidade de “APROVADO” ou se o status de conformidade mudar de “FALHOU” para “APROVADO”. Caso contrário, o Workflow.Status será “NOVO”. Você pode alterar esse valor com a operação BatchUpdateFindingsda API.

Interpretar o rótulo de gravidade

Todas as descobertas das avaliações de AWS Config regras têm um rótulo de severidade padrão de MEDIUM no ASFF. Você pode atualizar o rótulo de gravidade de uma descoberta com a operação `BatchUpdateFindings` da API.

Descoberta típica de AWS Config

O Security Hub transforma avaliações de AWS Config regras em descobertas que seguem o ASFF. A seguir está um exemplo de uma descoberta típica AWS Config do ASFF.

> **Note**
>
> Se a descrição tiver mais de 1024 caracteres, ela será truncada para 1024 caracteres e dirá “(truncada)” ao final.

```
{
 "SchemaVersion": "2018-10-08",
 "Id": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/45g070df80cb50b68fa6a43594kc6fda1e517932",
 "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/config",
```

```
 "ProductName": "Config",
 "CompanyName": "AWS",
 "Region": "eu-central-1",
 "GeneratorId": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-
mburzq",
 "AwsAccountId": "123456789012",
 "Types": [
  "Software and Configuration Checks"
 ],
 "CreatedAt": "2022-04-15T05:00:37.181Z",
 "UpdatedAt": "2022-04-19T21:20:15.056Z",
 "Severity": {
  "Label": "MEDIUM",
  "Normalized": 40
 },
 "Title": "s3-bucket-level-public-access-prohibited-config-integration-demo",
 "Description": "This finding is created for a resource compliance change for config
 rule: s3-bucket-level-public-access-prohibited-config-integration-demo",
 "ProductFields": {
  "aws/securityhub/ProductName": "Config",
  "aws/securityhub/CompanyName": "AWS",
  "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
config/arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/46f070df80cd50b68fa6a43594dc5fda1e517902",
  "aws/config/ConfigRuleArn": "arn:aws:config:eu-central-1:123456789012:config-rule/
config-rule-mburzq",
  "aws/config/ConfigRuleName": "s3-bucket-level-public-access-prohibited-config-
integration-demo",
  "aws/config/ConfigComplianceType": "NON_COMPLIANT"
 },
 "Resources": [{
  "Type": "AwsS3Bucket",
  "Id": "arn:aws:s3:::config-integration-demo-bucket",
  "Partition": "aws",
  "Region": "eu-central-1",
  "Details": {
   "AwsS3Bucket": {
    "OwnerId": "4edbba300f1caa608fba2aad2c8fcfe30c32ca32777f64451eec4fb2a0f10d8c",
    "CreatedAt": "2022-04-15T04:32:53.000Z"
   }
  }
 }],
 "Compliance": {
  "Status": "FAILED"
```

```
 },
 "WorkflowState": "NEW",
 "Workflow": {
  "Status": "NEW"
 },
 "RecordState": "ACTIVE",
 "FindingProviderFields": {
  "Severity": {
   "Label": "MEDIUM"
  },
  "Types": [
   "Software and Configuration Checks"
  ]
 }
}
```

Habilitar e configurar a integração

Depois de habilitar o Security Hub, essa integração é ativada automaticamente. AWS Config imediatamente começa a enviar as descobertas para o Security Hub.

Interromper a publicação de descobertas no Security Hub da

Para interromper o envio de descobertas ao Security Hub, você pode usar o console do Security Hub, a API do Security Hub ou o AWS CLI.

Consulte Desabilitar e habilitar o fluxo de descobertas em uma integração (console) ou Desabilitando o fluxo de descobertas de uma integração (API do Security Hub) AWS CLI.

AWS Firewall Manager (Envia descobertas)

O Firewall Manager envia descobertas para o Security Hub quando uma política de firewall de aplicativo Web (WAF) para recursos ou uma regra de lista de controle de acesso da web (ACL da Web) não está em conformidade. O Firewall Manager também envia descobertas quando não AWS Shield Advanced está protegendo recursos ou quando um ataque é identificado.

Depois de habilitar o Security Hub, essa integração é ativada automaticamente. O Firewall Manager começa imediatamente a enviar descobertas ao Security Hub.

Para saber mais sobre integração, veja a página Integrações no console do Security Hub.

Para saber mais sobre o Firewall Manager, consulte Guia do desenvolvedor do AWS WAF .

Amazon GuardDuty (envia descobertas)

GuardDuty envia todas as descobertas geradas para o Security Hub.

As novas descobertas GuardDuty são enviadas ao Security Hub em cinco minutos. As atualizações das descobertas são enviadas com base na configuração de descobertas atualizadas da Amazon EventBridge nas GuardDuty configurações.

Quando você gera GuardDuty amostras de descobertas usando a página GuardDuty Configurações, o Security Hub recebe as descobertas de amostra e omite o prefixo `[Sample]` no tipo de descoberta. Por exemplo, o tipo de descoberta de amostra em GuardDuty `[SAMPLE] Recon:IAMUser/ResourcePermissions` é exibido como `Recon:IAMUser/ResourcePermissions` no Security Hub.

Depois de habilitar o Security Hub, essa integração é ativada automaticamente. GuardDuty imediatamente começa a enviar as descobertas para o Security Hub.

Para obter mais informações sobre a GuardDuty integração, consulte Integração com o AWS Security Hub no Guia GuardDuty do usuário da Amazon.

AWS Health (Envia descobertas)

AWS Health fornece visibilidade contínua do desempenho de seus recursos e da disponibilidade de seus AWS serviços e contas. Você pode usar eventos do AWS Health para saber como as mudanças de serviços e recursos podem afetar seus aplicativos executados no AWS.

A integração com AWS Health não usa`BatchImportFindings`. Em vez disso, AWS Health usa mensagens de service-to-service eventos para enviar descobertas ao Security Hub.

Para mais informações sobre a integração, consulte as seções a seguir.

Como AWS Health envia descobertas para o Security Hub

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

O Security Hub fornece ferramentas para gerenciar descobertas em todas essas fontes. Você pode exibir e filtrar listas de descobertas e exibir detalhes de uma descoberta. Consulte Gerenciando e

revisando detalhes e histórico de busca. Você também pode rastrear o status de uma investigação em uma descoberta. Consulte Tomando medidas com base nas descobertas em AWS Security Hub.

Todas as descobertas no Security Hub usam um formato padrão JSON chamado AWS Formato de descoberta de segurança (ASFF). O ASFF inclui detalhes sobre a origem do problema, os recursos afetados e o status atual da descoberta.

AWS Health é um dos AWS serviços que envia descobertas para o Security Hub.

Tipos de descobertas que são AWS Health enviadas ao Security Hub

Depois que a integração estiver habilitada, AWS Health envia todas as descobertas relacionadas à segurança geradas para o Security Hub. As descobertas são enviadas para o Security Hub usando o AWS Formato de descoberta de segurança (ASFF). As descobertas relacionadas à segurança são definidas da seguinte forma:

- Qualquer descoberta associada a um serviço AWS de segurança
- Qualquer descoberta com as palavras`security`,`abuse`, ou `certificate` no AWS Health TypeCode
- Qualquer descoberta de onde está o AWS Health serviço `risk` ou `abuse`

Enviando AWS Health descobertas para o Security Hub

Quando você optar por aceitar as descobertas AWS Health, o Security Hub atribuirá automaticamente as permissões necessárias para receber as descobertas AWS Health. O Security Hub usa permissões de service-to-service nível que fornecem uma maneira fácil e segura de habilitar essa integração e importar descobertas AWS Health via Amazon EventBridge em seu nome. Escolher Aceitar descobertas concede ao Security Hub permissão para consumir descobertas de AWS Health.

Latência para enviar descobertas

Quando AWS Health cria uma nova descoberta, ela geralmente é enviada ao Security Hub em cinco minutos.

Tentar novamente quando o Security Hub não estiver disponível

AWS Health envia as descobertas para o Security Hub com base no melhor esforço, por meio de EventBridge. Quando um evento não é entregue com sucesso ao Security Hub, EventBridge tente enviar o evento novamente por 24 horas.

Atualizar as descobertas do existentes no Security Hub

Depois de AWS Health enviar uma descoberta para o Security Hub, ele pode enviar atualizações para a mesma descoberta para refletir observações adicionais da atividade de descoberta para o Security Hub.

Regiões nas quais existem descobertas

Para eventos globais, AWS Health envia as descobertas para o Security Hub em us-east-1 AWS (partição), cn-northwest-1 (partição da China) e -1 (partição). gov-us-west GovCloud AWS Health envia eventos específicos da região para o Security Hub na mesma região ou regiões em que os eventos ocorrem.

Visualizando AWS Health descobertas no Security Hub

Para ver suas AWS Health descobertas no Security Hub, escolha Descobertas no painel de navegação. Para filtrar as descobertas para exibir somente AWS Health as descobertas, escolha Health no campo Nome do produto.

Interpretando AWS Health encontrar nomes no Security Hub

AWS Health envia as descobertas para o Security Hub usando AWS Formato de descoberta de segurança (ASFF) o. AWS Health a descoberta usa um padrão de evento diferente em comparação com o formato ASFF do Security Hub. A tabela abaixo detalha todos os campos de AWS Health descoberta com seus equivalentes do ASFF conforme eles aparecem no Security Hub.

Tipo de descoberta de saúde	Tipo de descoberta do ASFF	Valor codificado
conta	AwsAccountId	
detail.startTime	CreatedAt	
detail.eventDescription.latestDescription	Descrição	
detalhe. eventTypeCode	GeneratorId	
Detail.eventArn (incluindo account) + hash de detail.startTime	Id	

Tipo de descoberta de saúde	Tipo de descoberta do ASFF	Valor codificado
"arn:aws:securityhub:<region>::product/aws/health"	ProductArn	
account ou resourceID	Resources[i].id	
	Resources[i].Type	“Outros”
	SchemaVersion	"2018-10-08"
	Severity.Label	Consulte “Interpretar o rótulo de gravidade” abaixo
Detalhe “AWS Health -”. eventTypeCode	Cargo	
-	Tipos	[“Verificações de Software e Configuração”]
event.time	UpdatedAt	
URL do evento no console de Saúde	SourceUrl	

Interpretar o rótulo de gravidade

O rótulo de gravidade na descoberta do ASFF é determinado usando a seguinte lógica:

- Gravidade CRÍTICA se:
  - O `service` campo na AWS Health descoberta tem o valor `Risk`
  - O `typeCode` campo na AWS Health descoberta tem o valor `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`
  - O `typeCode` campo na AWS Health descoberta tem o valor `AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK`
  - O `typeCode` campo na AWS Health descoberta tem o valor `AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES`

Gravidade ALTA se:

- O `service` campo na AWS Health descoberta tem o valor `Abuse`
- O `typeCode` campo na AWS Health descoberta contém o valor `SECURITY_NOTIFICATION`
- O `typeCode` campo na AWS Health descoberta contém o valor `ABUSE_DETECTION`

Gravidade MÉDIA se:

- O campo `service` na descoberta for qualquer um dos seguintes: `ACM`, `ARTIFACT`, `AUDITMANAGER`, `BACKUP`,`CLOUDENDURE`, `CLOUDHSM`, `CLOUDTRAIL`, `CLOUDWATCH`, `CODEGURGU`, `COGNITO`, `CONFIG`, `CONTROLTOWER`, `DETECTIVE`, `DIRECTORYSERVICE`, `DRS`, `EVENTS`, `FIREWALLMANAGER`, `GUARDDUTY`, `IAM`, `INSPECTOR`, `INSPECTOR2`, `IOTDEVICEDEFENDER`, `KMS`, `MACIE`, `NETWORKFIREWALL`, `ORGANIZATIONS`, `RESILIENCEHUB`, `RESOURCEMANAGER`, `ROUTE53`, `SECURITYHUB`, `SECRETSMANAGER`, `SES`, `SHIELD`, `SSO`, or `WAF`
- O campo typeCode na descoberta AWS Health contiver o valor de `CERTIFICATE`
- O campo typeCode na descoberta AWS Health contiver o valor de `END_OF_SUPPORT`

Descoberta típica de AWS Health

AWS Health envia as descobertas para o Security Hub usando AWS Formato de descoberta de segurança (ASFF) o. A seguir está um exemplo de uma descoberta típica de AWS Health.

> **Note**
>
> Se a descrição tiver mais de 1024 caracteres, ela será truncada para 1024 caracteres e dirá (truncada) ao final.


```
{
            "SchemaVersion": "2018-10-08",
            "Id": "arn:aws:health:us-east-1:123456789012:event/SES/
AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-
b533-78e29f49de96/101F7FBAEFC663977DA09CFF56A29236602834D2D361E6A8CA5140BFB3A69B30",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/health",
            "GeneratorId": "AWS_SES_CMF_PENDING_TO_SUCCESS",
            "AwsAccountId": "123456789012",
            "Types": [
                "Software and Configuration Checks"
```

```
            ],
            "CreatedAt": "2022-01-07T16:34:04.000Z",
            "UpdatedAt": "2022-01-07T19:17:43.000Z",
            "Severity": {
                "Label": "MEDIUM",
                "Normalized": 40
            },
            "Title": "AWS Health - AWS_SES_CMF_PENDING_TO_SUCCESS",
            "Description": "Congratulations! Amazon SES has successfully detected the
 MX record required to use 4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com as a custom MAIL FROM domain for verified identity cmf.pinpoint.sysmon-
iad.adzel.com in AWS Region US East (N. Virginia).\\n\\nYou can now use this MAIL
 FROM domain with cmf.pinpoint.sysmon-iad.adzel.com and any other verified identity
 that is configured to use it. For information about how to configure a verified
 identity to use a custom MAIL FROM domain, see http://docs.aws.amazon.com/ses/latest/
DeveloperGuide/mail-from-set.html .\\n\\nPlease note that this email only applies to
 AWS Region US East (N. Virginia).",
            "SourceUrl": "https://phd.aws.amazon.com/phd/home#/event-log?
eventID=arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
            "ProductFields": {
                "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
aws/health/arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
                "aws/securityhub/ProductName": "Health",
                "aws/securityhub/CompanyName": "AWS"
            },
            "Resources": [
                {
                    "Type": "Other",
                    "Id": "4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com"
                }
            ],
            "WorkflowState": "NEW",
            "Workflow": {
                "Status": "NEW"
            },
            "RecordState": "ACTIVE",
            "FindingProviderFields": {
                "Severity": {
                    "Label": "MEDIUM"
                },
                "Types": [
```

```
                    "Software and Configuration Checks"
                ]
            }
        }
    ]
}
```

Habilitar e configurar a integração

Depois de habilitar o Security Hub, essa integração é ativada automaticamente. AWS Health imediatamente começa a enviar as descobertas para o Security Hub.

Interromper a publicação de descobertas no Security Hub da

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

Consulte Desabilitar e habilitar o fluxo de descobertas em uma integração (console) ou Desabilitando o fluxo de descobertas de uma integração (API do Security Hub) AWS CLI.

AWS Identity and Access Management Access Analyzer (Envia descobertas)

Com o IAM Access Analyzer, todas as descobertas são enviadas para o Security Hub.

O IAM Access Analyzer usa raciocínio baseado em lógica para analisar políticas baseadas em recursos aplicadas a recursos compatíveis em sua conta. O IAM Access Analyzer gera uma descoberta quando detecta uma instrução de política que permite que uma entidade principal externa acesse um recurso em sua conta.

No IAM Access Analyzer, apenas a conta do administrador pode ver as descobertas dos analisadores que se aplicam a uma organização. Para analisadores da organização, o campo do ASFF `AwsAccountId` reflete o ID da conta do administrador. Em `ProductFields`, o campo `ResourceOwnerAccount` indica a conta onde a descoberta foi encontrada Se você habilitar analisadores individualmente para cada conta, o Security Hub gerará várias descobertas, uma que identifica a ID da conta do administrador e outra que identifica a ID da conta do recurso.

Para obter mais informações, consulte Integração com o Security Hub do AWS no Guia do usuário do IAM.

Amazon Inspector (envia descobertas)

O Amazon Inspector é um serviço de gerenciamento de vulnerabilidade que verifica continuamente suas worloads AWS em busca de vulnerabilidades. O Amazon Inspector descobre e escaneia automaticamente instâncias do Amazon EC2 e imagens de contêiner que residem no Amazon Elastic Container Registry. O escaneamento busca vulnerabilidades de software e exposição não intencional da rede.

Depois de habilitar o Security Hub, essa integração é ativada automaticamente. O Amazon Inspector começa imediatamente a enviar todas as descobertas geradas para o Security Hub.

Para obter mais informações sobre a integração, consulte Integração com o AWS Security Hub no Guia do Usuário do Amazon Inspector.

O Security Hub também pode receber descobertas do Amazon Inspector Classic. O Amazon Inspector Classic envia descobertas ao Security Hub que são geradas por meio de execuções de avaliação para todos os pacotes de regras compatíveis.

Para obter mais informações sobre a integração, consulte Integração com o AWS Security Hub no Guia do usuário do Amazon Inspector Classic.

As descobertas do Amazon Inspector e do Amazon Inspector Classic usam o mesmo ARN do produto. As descobertas do Amazon Inspector têm a seguinte entrada em `ProductFields`:

```
"aws/inspector/ProductVersion": "2",
```

AWS IoT Device Defender (Envia descobertas)

AWS IoT Device Defender é um serviço de segurança que audita a configuração de seus dispositivos de IoT, monitora dispositivos conectados para detectar comportamentos anormais e ajuda a reduzir os riscos de segurança.

Depois de ativar o Security Hub AWS IoT Device Defender e o Security Hub, visite a página Integrações do console do Security Hub e escolha Aceitar descobertas para Auditoria, Detecção ou ambos. AWS IoT Device Defender O Audit and Detect começa a enviar todas as descobertas para o Security Hub.

AWS IoT Device Defender A auditoria envia resumos de verificação para o Security Hub, que contêm informações gerais para um tipo específico de verificação de auditoria e tarefa de auditoria. AWS IoT

Device Defender O Detect envia descobertas de violações para comportamentos de aprendizado de máquina (ML), estatísticos e estáticos para o Security Hub. Auditar também envia atualizações de descoberta para o Security Hub.

Para obter mais informações sobre essa integração, consulte Integração com o AWS Security Hub no Guia do AWS IoT desenvolvedor.

Amazon Macie (envia descobertas)

Uma descoberta do Macie pode indicar que há uma possível violação de política ou que dados confidenciais, como informações de identificação pessoal (PII), estão presentes nos dados que sua organização armazena no Amazon S3.

Depois de o Security Hub ser habilitado, o Macie começa automaticamente a enviar as descobertas da política para o Security Hub. A integração com o Macie pode ser configurada para também enviar descobertas de dados confidenciais ao Security Hub.

No Security Hub, o tipo de descoberta de uma política ou de dados confidenciais é alterado para um valor compatível com o ASFF. Por exemplo, o tipo de descoberta no Macie do `Policy:IAMUser/S3BucketPublic` é exibido como no Security Hub `Effects/Data Exposure/Policy:IAMUser-S3BucketPublic`.

O Macie também envia descobertas de amostras geradas pelo Security Hub. Para exemplos de descobertas, o nome do recurso afetado é `macie-sample-finding-bucket` e o valor do campo `Sample` é`true`.

Para obter mais informações, consulte Integração do Amazon Macie com o AWS Security Hub no Guia do usuário do Amazon Macie.

AWS Systems Manager Gerenciador de patches (envia descobertas)

AWS Systems Manager O Patch Manager envia as descobertas para o Security Hub quando as instâncias da frota de um cliente não estão em conformidade com o padrão de conformidade de patches.

O Patch Manager automatiza o processo de instâncias de patch gerenciadas com atualizações relacionadas à segurança e outros tipos de atualizações.

Depois de habilitar o Security Hub, essa integração é ativada automaticamente. O Systems Manager Patch Manage começa imediatamente a enviar descobertas ao Security Hub.

Para obter mais informações sobre como usar o Patch Manager, consulte Patch Manager do AWS Systems Manager no AWS Systems Manager Guia do usuário.

AWS serviços que recebem descobertas do Security Hub

Os AWS serviços a seguir são integrados ao Security Hub e recebem descobertas do Security Hub. Onde observado, o serviço integrado também pode atualizar as descobertas. Nesse caso, as atualizações de descoberta feitas no serviço integrado também serão refletidas no Security Hub.

AWS Audit Manager (Recebe descobertas)

AWS Audit Manager recebe descobertas do Security Hub. Essas descobertas ajudam os usuários do Audit Manager a se preparar para as auditorias.

Para saber mais sobre o Audit Manager, consulte o Guia do usuário do AWS Audit Manager. AWS As verificações do Security Hub compatíveis com AWS Audit Manager listam os controles para os quais o Security Hub envia as descobertas ao Audit Manager.

AWS Chatbot (Recebe descobertas)

AWS Chatbot é um agente interativo que ajuda você a monitorar e interagir com seus AWS recursos nos canais do Slack e nas salas de bate-papo do Amazon Chime.

AWS Chatbot recebe descobertas do Security Hub.

Para saber mais sobre a AWS Chatbot integração com o Security Hub, consulte a visão geral da integração com o Security Hub no Guia AWS Chatbot do Administrador.

Amazon Detective (recebe descobertas)

Detective coleta automaticamente dados de registro de seus AWS recursos e usa aprendizado de máquina, análise estatística e teoria dos gráficos para ajudá-lo a visualizar e conduzir investigações de segurança mais rápidas e eficientes.

A integração do Security Hub com o Detective permite que você passe das descobertas da GuardDuty Amazon no Security Hub para o Detective. Você pode então usar as ferramentas e visualizações do Detective para investigá-las. A integração não requer nenhuma configuração adicional no Security Hub ou Detective.

Para descobertas recebidas de outros Serviços da AWS, o painel de detalhes da descoberta no console do Security Hub inclui uma subseção Investigue em Detective. Essa subseção contém um

link para o Detective, onde você pode investigar mais detalhadamente o problema de segurança que a descoberta sinalizou. Você também pode criar um gráfico de comportamento no Detective com base nas descobertas do Security Hub para conduzir investigações mais eficazes. Para obter mais informações, consulte descobertas de segurança do AWS no Guia de administração do Amazon Detective.

Se a agregação entre regiões for ativada, quando você sair da região de agregação, o Detective será aberto na região de origem da descoberta.

Se um link não funcionar, para obter orientações de solução de problemas, consulte Solução de problemas de alternância.

Amazon Security Lake (recebe descobertas)

O Security Lake é um serviço de data lake de segurança totalmente gerenciado. O Security Lake pode ser usado para centralizar automaticamente dados de segurança da nuvem, on-premises e fontes personalizadas em um data lake armazenado em sua conta. Os assinantes podem consumir dados do Security Lake para casos de uso investigativos e analíticos.

Para ativar essa integração, você deve habilitar os dois serviços e adicionar o Security Hub como fonte no console do Security Lake, na API do Security Lake ou AWS CLI. Depois de executar essas etapas, o Security Hub começa a enviar todas as descobertas para o Security Lake.

O Security Lake normaliza automaticamente as descobertas do Security Hub e as converte em um esquema padronizado de código aberto chamado Open Cybersecurity Schema Framework (OCSF). No Security Lake, você pode adicionar um ou mais assinantes para consumir as descobertas do Security Hub.

Para obter mais informações sobre essa integração, incluindo instruções sobre como adicionar o Security Hub como fonte e criar assinantes, consulte Integração com o AWS Security Hub no Guia do usuário do Amazon Security Lake.

AWS Systems Manager Explorer e OpsCenter (recebe e atualiza as descobertas)

AWS Systems Manager Explore e OpsCenter receba descobertas do Security Hub e atualize essas descobertas no Security Hub.

O Explorer traz um painel personalizável, fornecendo informações e análises importantes sobre a integridade operacional e o desempenho do seu ambiente AWS .

OpsCenter fornece um local central para visualizar, investigar e resolver itens de trabalho operacionais.

Para obter mais informações sobre o Explorer e OpsCenter, consulte Gerenciamento de operações no Guia AWS Systems Manager do Usuário.

AWS Trusted Advisor (Recebe descobertas)

Trusted Advisor baseia-se nas melhores práticas aprendidas ao atender centenas de milhares de AWS clientes. Trusted Advisor inspeciona seu AWS ambiente e, em seguida, faz recomendações quando existem oportunidades para economizar dinheiro, melhorar a disponibilidade e o desempenho do sistema ou ajudar a fechar lacunas de segurança.

Quando você ativa o Security Hub Trusted Advisor e o Security Hub, a integração é atualizada automaticamente.

O Security Hub envia os resultados de suas AWS verificações de melhores práticas de segurança básica para Trusted Advisor.

Para obter mais informações sobre a integração do Security Hub com Trusted Advisor, consulte Visualizando os controles do AWS Security Hub AWS Trusted Advisor no AWS Support User Guide.

Integrações de produtos de parceiros terceirizados disponíveis

AWS O Security Hub se integra a vários produtos de parceiros terceirizados. Uma integração pode realizar uma ou mais das seguintes ações:

- Enviar descobertas que gera para o Security Hub.
- Receber descobertas do Security Hub.
- Atualizar descobertas no Security Hub.

Todas as integrações que enviam descobertas para o Security Hub têm um nome do recurso da Amazon (ARN).

> **Note**
>
> Algumas integrações só estão disponíveis em select Regiões da AWS.
> A página Integrações do console do Security Hub lista todas as integrações compatíveis para a região atual.

Para obter mais informações, consulte Integrações com suporte na China (Pequim) e na China (Ningxia) e Integrações que são suportadas em AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA).

Se você tiver uma solução de segurança e estiver interessado em se tornar um parceiro do Security Hub, envie um email para <securityhub-partners@amazon.com>. Para obter mais informações, consulte o Guia de integração de parceiros do AWS Security Hub.

Visão geral das integrações de terceiros com o Security Hub

Aqui está uma visão geral das integrações de terceiros que enviam descobertas para o Security Hub ou recebem descobertas do Security Hub.

Integração	Direction	ARN (se aplicável)
3CORESec – 3CORESec NTA	Envia descobertas	`arn:aws:securityhub: <REGION>::product/3coresec/3coresec`
Alert Logic – SIEMless Threat Management	Envia descobertas	`arn:aws:securityhub: <REGION>:733251395267:product/alertlogic/althreatmanagement`
Aqua Security – Aqua Cloud Native Security Platform	Envia descobertas	`arn:aws:securityhub: <REGION>::product/aquasecurity/aquasecurity`
Aqua Security – Kube-bench	Envia descobertas	`arn:aws:securityhub: <REGION>::product/aqua-security/kube-bench`
Armor – Armor Anywhere	Envia descobertas	`arn:aws:securityhub: <REGION>:67970361`

Integração	Direction	ARN (se aplicável)
		5338:product/armor defense/armoranywh ere
AttackIQ – AttackIQ	Envia descobertas	arn:aws:securityhu b: *<REGION>*::product /attackiq/attackiq- platform
Barracuda Networks – Cloud Security Guardian	Envia descobertas	arn:aws:securityhu b: *<REGION>*:15178405 5945:product/barra cuda/cloudsecurity guardian
BigID – BigID Enterprise	Envia descobertas	arn:aws:securityhu b: *<REGION>*::product /bigid/bigid-enter prise
Blue Hexagon – Blue Hexagon forAWS	Envia descobertas	arn:aws:securityhu b: *<REGION>*::product /blue-hexagon/blue- hexagon-for-aws
Capitis Solutions – C2VS	Envia descobertas	arn:aws:securityhu b: *<REGION>*::product/ capitis/c2vs
Check Point – CloudGuard IaaS	Envia descobertas	arn:aws:securityhu b: *<REGION>*:75824556 3457:product/check point/cloudguard-i aas

Integração	Direction	ARN (se aplicável)
Check Point – CloudGuard Posture Management	Envia descobertas	`arn:aws:securityhub: <REGION>:634729597623:product/checkpoint/dome9-arc`
Claroty – xDome	Envia descobertas	`arn:aws:securityhub: <REGION>::product/claroty/xdome`
Cloud Storage Security: Antivirus for Amazon S3	Envia descobertas	`arn:aws:securityhub: <REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`
Contrast Security	Envia descobertas	`arn:aws:securityhub: <REGION>::product/contrast-security/security-assess`
CrowdStrike – CrowdStrike Falcon	Envia descobertas	`arn:aws:securityhub: <REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`
CyberArk – Privileged Threat Analytics	Envia descobertas	`arn:aws:securityhub: <REGION>:749430749651:product/cyberark/cyberark-pta`
Data Theorem – Data Theorem	Envia descobertas	`arn:aws:securityhub: <REGION>::product/data-theorem/api-cloud-web-secure`

Integração	Direction	ARN (se aplicável)
Drata	Envia descobertas	`arn:aws:securityhub: <REGION>::product/drata/drata-integration`
Forcepoint – Forcepoint CASB	Envia descobertas	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-casb`
Forcepoint – Forcepoint Cloud Security Gateway	Envia descobertas	`arn:aws:securityhub: <REGION>::product/forcepoint/forcepoint-cloud-security-gateway`
Forcepoint – Forcepoint DLP	Envia descobertas	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-dlp`
Forcepoint – Forcepoint NGFW	Envia descobertas	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-ngfw`
Fugue – Fugue	Envia descobertas	`arn:aws:securityhub: <REGION>::product/fugue/fugue`

Integração	Direction	ARN (se aplicável)
Guardicore – Centra 4.0	Envia descobertas	`arn:aws:securityhub: <REGION>::product/guardicore/guardicore`
HackerOne – Vulnerability Intelligence	Envia descobertas	`arn:aws:securityhub: <REGION>::product/hackerone/vulnerability-intelligence`
JFrog – Xray	Envia descobertas	`arn:aws:securityhub: <REGION>::product/jfrog/jfrog-xray`
Juniper Networks – vSRX Next Generation Firewall	Envia descobertas	`arn:aws:securityhub: <REGION>::product/juniper-networks/vsrx-next-generation-firewall`
k9 Security – Access Analyzer	Envia descobertas	`arn:aws:securityhub: <REGION>::product/k9-security/access-analyzer`
Lacework – Lacework	Envia descobertas	`arn:aws:securityhub: <REGION>::product/lacework/lacework`
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	Envia descobertas	`arn:aws:securityhub: <REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

Integração	Direction	ARN (se aplicável)
NETSCOUT – NETSCOUT Cyber Investigator	Envia descobertas	`arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator`
Palo Alto Networks – Prisma Cloud Compute	Envia descobertas	`arn:aws:securityhub: <REGION>:496947949261:product/twistlock/twistlock-enterprise`
Palo Alto Networks – Prisma Cloud Enterprise	Envia descobertas	`arn:aws:securityhub: <REGION>:188619942792:product/paloaltonetworks/redlock`
Plerion – Cloud Security Platform	Envia descobertas	`arn:aws:securityhub: <REGION>::product/plerion/cloud-security-platform`
Prowler – Prowler	Envia descobertas	`arn:aws:securityhub: <REGION>::product/prowler/prowler`
Qualys – Vulnerability Management	Envia descobertas	`arn:aws:securityhub: <REGION>:805950163170:product/qualys/qualys-vm`
Rapid7 – InsightVM	Envia descobertas	`arn:aws:securityhub: <REGION>:336818582268:product/rapid7/insightvm`

Integração	Direction	ARN (se aplicável)
SecureCloudDB – SecureCloudDB	Envia descobertas	`arn:aws:securityhub: <REGION>::product/securecloudb/securecloudb`
SentinelOne – SentinelOne	Envia descobertas	`arn:aws:securityhub: <REGION>::product/sentinelone/endpoint-protection`
Snyk	Envia descobertas	`arn:aws:securityhub: <region>::product/snyk/snyk`
Sonrai Security – Sonrai Dig	Envia descobertas	`arn:aws:securityhub: <REGION>::product/sonrai-security/sonrai-dig`
Sophos – Server Protection	Envia descobertas	`arn:aws:securityhub: <REGION>:062897671886:product/sophos/sophos-server-protection`
StackRox – StackRox Kubernetes Security	Envia descobertas	`arn:aws:securityhub: <REGION>::product/stackrox/kubernetes-security`
Sumo Logic – Machine Data Analytics	Envia descobertas	`arn:aws:securityhub: <REGION>:956882708938:product/sumologicinc/sumologic-mda`

Integração	Direction	ARN (se aplicável)
Symantec – Cloud Workload Protection	Envia descobertas	`arn:aws:securityhub: <REGION>:754237914691:product/symantec-corp/symantec-cwp`
Tenable – Tenable.io	Envia descobertas	`arn:aws:securityhub: <REGION>:422820575223:product/tenable/tenable-io`
Trend Micro – Cloud One	Envia descobertas	`arn:aws:securityhub: <REGION>::product/trend-micro/cloud-one`
Vectra – Cognito Detect	Envia descobertas	`arn:aws:securityhub: <REGION>:978576646331:product/vectra-ai/cognito-detect`
Wiz	Envia descobertas	`arn:aws:securityhub: <REGION>::product/wiz-security/wiz-security`
Atlassian - Jira Service Management	Recebe e atualiza as descobertas	Não aplicável
Atlassian - Jira Service Management Cloud	Recebe e atualiza as descobertas	Não aplicável
Atlassian – Opsgenie	Recebe descobertas	Não aplicável
Fortinet – FortiCNP	Recebe descobertas	Não aplicável
IBM – QRadar	Recebe descobertas	Não aplicável

Integração	Direction	ARN (se aplicável)
Logz.io Cloud SIEM	Recebe descobertas	Não aplicável
MetricStream	Recebe descobertas	Não aplicável
MicroFocus – MicroFocus Arcsight	Recebe descobertas	Não aplicável
New Relic Vulnerability Management	Recebe descobertas	Não aplicável
PagerDuty – PagerDuty	Recebe descobertas	Não aplicável
Palo Alto Networks – Cortex XSOAR	Recebe descobertas	Não aplicável
Palo Alto Networks – VM-Series	Recebe descobertas	Não aplicável
Rackspace Technology – Cloud Native Security	Recebe descobertas	Não aplicável
Rapid7 – InsightConnect	Recebe descobertas	Não aplicável
RSA – RSA Archer	Recebe descobertas	Não aplicável
ServiceNow – ITSM	Recebe e atualiza as descobertas	Não aplicável
Slack – Slack	Recebe descobertas	Não aplicável
Splunk – Splunk Enterprise	Recebe descobertas	Não aplicável
Splunk – Splunk Phantom	Recebe descobertas	Não aplicável
ThreatModeler	Recebe descobertas	Não aplicável
Trellix – Trellix Helix	Recebe descobertas	Não aplicável

Integração	Direction	ARN (se aplicável)
Caveonix – Caveonix Cloud	Envia e recebe descobertas	`arn:aws:securityhub: <REGION>::product/caveonix/caveonix-cloud`
Cloud Custodian – Cloud Custodian	Envia e recebe descobertas	`arn:aws:securityhub: <REGION>::product/cloud-custodian/cloud-custodian`
DisruptOps, Inc. – DisruptOPS	Envia e recebe descobertas	`arn:aws:securityhub: <REGION>::product/disruptops-inc/disruptops`
Kion	Envia e recebe descobertas	`arn:aws:securityhub: <REGION>::product/cloudtamerio/cloudtamerio`
Turbot – Turbot	Envia e recebe descobertas	`arn:aws:securityhub: <REGION>:453761072151:product/turbot/turbot`

Integrações de terceiros que enviam descobertas para o Security Hub

As seguintes integrações de produtos de parceiros terceirizados enviam descobertas para o Security Hub. O Security Hub transforma as descobertas para o AWS Formato do Security Finding.

3CORESec – 3CORESec NTA

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/3coresec/3coresec`

3CORESec fornece serviços gerenciados de detecção tanto para sistemas on-premises quanto para sistemas da AWS . Sua integração com o Security Hub permite a visibilidade de ameaças como malware, escalonamento de privilégios, movimentação lateral e segmentação imprópria da rede.

Link do produto

Documentação do parceiro

Alert Logic – SIEMless Threat Management

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement`

Obtenha o nível certo de cobertura: visibilidade de vulnerabilidade e ativos, detecção de ameaças e gerenciamento de incidentes e opções atribuídas aos analistas de SOC. AWS WAF

Link do produto

Documentação do parceiro

Aqua Security – Aqua Cloud Native Security Platform

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

A Aqua Cloud Native Security Platform (CSP) fornece segurança em todo o ciclo de vida para aplicativos baseados em contêiner e tecnologia sem servidor, desde seu pipeline de CI/CD até ambientes de produção em runtime.

Link do produto

Documentação do parceiro

Aqua Security – Kube-bench

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-bench é uma ferramenta de código aberto que executa a referência de Kubernetes do Center for Internet Security (CIS) em seu ambiente.

Link do produto

Documentação do parceiro

Armor – Armor Anywhere

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywhereoferece segurança e conformidade gerenciadas para AWS.

Link do produto

Documentação do parceiro

AttackIQ – AttackIQ

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

A AttackIQ Platform emula comportamentos adversários reais alinhados à estrutura MITRE ATT&CK para ajudar a validar e melhorar sua postura de segurança geral.

Link do produto

Documentação do parceiro

Barracuda Networks – Cloud Security Guardian

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

O Barracuda Cloud Security Sentry ajuda as organizações a permanecerem seguras enquanto criam aplicativos e movem as wokloads para a nuvem pública.

AWS Link do Marketplace

Link do produto

BigID – BigID Enterprise

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

A BigID Enterprise Privacy Management Platform ajuda as empresas a gerenciar e proteger dados confidenciais (PII) em todos os seus sistemas.

Link do produto

Documentação do parceiro

Blue Hexagon— Blue Hexagon para AWS

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagon é uma plataforma de detecção de ameaças em tempo real. Ela usa princípios de aprendizado profundo para detectar ameaças conhecidas e desconhecidas, incluindo malware e anomalias de rede.

AWS Link do Marketplace

Documentação do parceiro

Capitis Solutions – C2VS

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/capitis/c2vs`

O C2VS é uma solução de conformidade personalizável projetada para identificar automaticamente as configurações incorretas específicas do aplicativo e a causa-raiz.

Link do produto

Documentação do parceiro

Check Point – CloudGuard IaaS

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuardestende facilmente a segurança abrangente de prevenção de ameaças e, ao AWS mesmo tempo, protege os ativos na nuvem.

Link do produto

Documentação do parceiro

Check Point – CloudGuard Posture Management

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

Uma plataforma SaaS que oferece segurança de rede em nuvem verificável, proteção avançada do IAM e conformidade e governança abrangentes.

Link do produto

Documentação do parceiro

Claroty – xDome

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/claroty/xdome`

o Claroty xDome ajuda as organizações a proteger seus sistemas ciberfísicos na Extended Internet of Things (XIoT) em ambientes industriais (OT), de saúde (IoMT) e corporativos (IoT).

Link do produto

Documentação do parceiro

Cloud Storage Security: Antivirus for Amazon S3

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

A Cloud Storage Security fornece escaneamento antimalware e antivírus nativo de nuvem para objetos do Amazon S3.

O Antivirus for Amazon S3 oferece varreduras programadas e em tempo real de objetos e arquivos no Amazon S3 em busca de malware e ameaças. Ele fornece visibilidade e correção de problemas e arquivos infectados.

Link do produto

Documentação do parceiro

Contrast Security – Contrast Assess

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

O Contrast Security Contrast Assess é uma ferramenta IAST que oferece detecção de vulnerabilidade em tempo real em aplicativos web, APIs e microsserviços. O Contrast Assess se integra ao Security Hub para ajudar a fornecer visibilidade e resposta centralizadas para todas as workloads.

Link do produto

Documentação do parceiro

CrowdStrike – CrowdStrike Falcon

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

O sensor leve único do CrowdStrike Falcon unifica antivírus de última geração, detecção e resposta de endpoint e busca gerenciada 24 horas por dia, 7 dias por semana por meio da nuvem.

Link do produto

Documentação do parceiro

CyberArk – Privileged Threat Analytics

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

O Privileged Threat Analytics coleta, detecta, alerta e responde a atividades de alto risco e ao comportamento de contas privilegiadas para conter ataques em andamento.

Link do produto

Documentação do parceiro

Data Theorem – Data Theorem

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure`

Data Theoremexamina continuamente aplicativos da web, APIs e recursos de nuvem em busca de falhas de segurança e lacunas na privacidade de dados para evitar AppSec violações de dados.

Link do produto

Documentação do parceiro

Drata

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/drata/drata-integration`

O Drata é uma plataforma de automação de conformidade que ajuda você a alcançar e manter a conformidade com várias estruturas, como SOC2, ISO e GDPR. A integração entre o Drata e o Security Hub ajuda você a centralizar suas descobertas de segurança em um único local.

AWS Link do Marketplace

Documentação do parceiro

Forcepoint – Forcepoint CASB

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

O Forcepoint CASB permite que você descubra o uso de aplicativos na nuvem, analise riscos e aplique controles apropriados para SaaS e aplicativos personalizados.

Link do produto

Documentação do parceiro

Forcepoint – Forcepoint Cloud Security Gateway

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

O Forcepoint Cloud Security Gateway é um serviço de segurança em nuvem convergente que fornece visibilidade, controle e proteção contra ameaças para usuários e dados, onde quer que estejam.

Link do produto

Documentação do parceiro

Forcepoint – Forcepoint DLP

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

O Forcepoint DLP aborda o risco humano com visibilidade e controle em qualquer lugar onde seus funcionários trabalhem e em qualquer lugar onde seus dados estejam.

Link do produto

Documentação do parceiro

Forcepoint – Forcepoint NGFW

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFWpermite que você conecte seu AWS ambiente à sua rede corporativa com a escalabilidade, a proteção e os insights necessários para gerenciar sua rede e responder às ameaças.

Link do produto

Documentação do parceiro

Fugue – Fugue

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/fugue/fugue`

Fugueé uma plataforma nativa da nuvem escalável e sem agentes que automatiza a validação contínua infrastructure-as-code e os ambientes de tempo de execução da nuvem usando as mesmas políticas.

Link do produto

Documentação do parceiro

Guardicore – Centra 4.0

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

O Guardicore Centra fornece visualização de fluxo, microssegmentação e detecção de violações para workloads em nuvens e datacenters modernos.

Link do produto

Documentação do parceiro

HackerOne – Vulnerability Intelligence

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

A plataforma HackerOne faz parceria com a comunidade global de hackers para descobrir os problemas de segurança mais relevantes. A Vulnerability Intelligence permite que sua organização vá além da digitalização automatizada. Ela compartilha vulnerabilidades que hackers éticos HackerOne validaram e forneceram etapas para reproduzir.

AWS link de mercado

Documentação do parceiro

JFrog – Xray

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

O JFrog Xray é uma ferramenta universal de Análise de composição de software (SCA) de segurança de aplicativos que verifica continuamente os binários em busca de vulnerabilidades de segurança e conformidade de licenças para que você possa executar uma cadeia de suprimentos de software segura.

AWS Link do Marketplace

Documentação do parceiro

Juniper Networks – vSRX Next Generation Firewall

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

O vSRX Virtual Next Generation Firewall da Juniper Networks' oferece um firewall virtual completo baseado em nuvem com segurança avançada, SD-WAN segura, rede robusta e automação integrada.

AWS Link do Marketplace

Documentação do parceiro

Link do produto

k9 Security – Access Analyzer

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Securitynotifica você quando mudanças importantes de acesso ocorrem em sua AWS Identity and Access Management conta. Com issok9 Security, você pode entender o acesso que os usuários e as funções do IAM têm aos dados essenciais Serviços da AWS e aos seus dados.

k9 Securityfoi criado para entrega contínua, permitindo que você operacionalize o IAM com auditorias de acesso acionáveis e automação simples de políticas para o Terraform. AWS CDK

Link do produto

Documentação do parceiro

Lacework – Lacework

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/lacework/lacework`

Lacework é a plataforma de segurança baseada em dados para a nuvem. A plataforma de segurança de nuvem da Lacework automatiza a segurança na nuvem em grande escala para que você possa inovar com velocidade e segurança.

Link do produto

Documentação do parceiro

McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

A McAfee MVISION Cloud Native Application Protection Platform (CNAPP) oferece Cloud Security Posture Management (CSPM) e Cloud Workload Protection Platform (CWPP) para seu ambiente da AWS .

Link do produto

Documentação do parceiro

NETSCOUT – NETSCOUT Cyber Investigator

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator`

O NETSCOUT Cyber Investigator é uma plataforma corporativa contra ameaças à rede, investigação de riscos e análise forense que ajuda a reduzir o impacto das ameaças cibernéticas nas empresas.

Link do produto

Documentação do parceiro

Palo Alto Networks – Prisma Cloud Compute

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

O Prisma Cloud Compute é uma plataforma de segurança cibernética nativa de nuvem que protege VMs, contêineres e plataformas sem servidor.

Link do produto

Documentação do parceiro

Palo Alto Networks – Prisma Cloud Enterprise

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

Protege sua AWS implantação com análises de segurança na nuvem, detecção avançada de ameaças e monitoramento de conformidade.

Link do produto

Documentação do parceiro

Plerion – Cloud Security Platform

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

O Plerion é uma plataforma de segurança em nuvem com uma abordagem exclusiva orientada por ameaças e riscos que oferece ações de prevenção, detecção e correção em todas as suas workloads. A integração entre o Plerion e o Security Hub permite que os clientes centralizem e ajam de acordo com suas descobertas de segurança em um só lugar.

AWS Link do Marketplace

Documentação do parceiro

Prowler – Prowler

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowleré uma ferramenta de segurança de código aberto para realizar AWS verificações relacionadas às melhores práticas de segurança, fortalecimento e monitoramento contínuo.

Link do produto

Documentação do parceiro

Qualys – Vulnerability Management

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

O Qualys Vulnerability Management (VM) verifica e identifica continuamente vulnerabilidades, protegendo seus ativos.

Link do produto

Documentação do parceiro

Rapid7 – InsightVM

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

O Rapid7 InsightVM fornece gerenciamento de vulnerabilidade para ambientes modernos, permitindo que você encontre, priorize e corrija eficientemente as vulnerabilidades.

Link do produto

Documentação do parceiro

SecureCloudDB – SecureCloudDB

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/securecloudb/securecloudb`

O SecureCloudDB é uma ferramenta de segurança de banco de dados nativa de nuvem que fornece visibilidade abrangente das posturas e atividades de segurança internas e externas. Ele sinaliza violações de segurança e fornece soluções para vulnerabilidades de banco de dados que podem ser exploradas.

Link do produto

Documentação do parceiro

SentinelOne – SentinelOne

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

O SentinelOne é uma plataforma autônoma de detecção e resposta estendida (XDR) que abrange prevenção, detecção, resposta e busca baseadas em IA em endpoints, contêineres, workloads na nuvem e dispositivos de IoT.

AWS Link do Marketplace

Link do produto

Snyk

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/snyk/snyk`

O Snyk fornece uma plataforma de segurança que escaneia os componentes do aplicativo em busca de riscos de segurança nas workloads em execução na AWS. Esses riscos são enviados ao Security Hub como descobertas, ajudando desenvolvedores e equipes de segurança a visualizá-los e priorizá-los junto com o restante de suas AWS descobertas de segurança.

AWS Link do Marketplace

Documentação do parceiro

Sonrai Security – Sonrai Dig

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

O Sonrai Dig monitora e corrige configurações incorretas e violações de políticas na nuvem, para que você possa melhorar sua postura de segurança e conformidade.

Link do produto

Documentação do parceiro

Sophos – Server Protection

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protectiondefende os aplicativos e dados essenciais no centro de sua organização, usando defense-in-depth técnicas abrangentes.

Link do produto

Documentação do parceiro

StackRox – StackRox Kubernetes Security

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

O StackRox ajuda as empresas a proteger as implantações de contêineres e Kubernetes em grande escala, aplicando as políticas de conformidade e segurança em todo o ciclo de vida do contêiner: criação, implantação e execução.

Link do produto

Documentação do parceiro

Sumo Logic – Machine Data Analytics

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

O Sumo Logic é uma plataforma segura de análise de dados de máquina que permite que as equipes do DevSecOps criem, executem e protejam os aplicativos da AWS .

Link do produto

Documentação do parceiro

Symantec – Cloud Workload Protection

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

O Cloud Workload Protection fornece proteção completa para suas instâncias do Amazon EC2 com antimalware, prevenção de intrusões e monitoramento de integridade de arquivos.

Link do produto

Documentação do parceiro

Tenable – Tenable.io

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

Identifique, investigue e priorize com precisão as vulnerabilidades. Managed in the Cloud.

Link do produto

Documentação do parceiro

Trend Micro – Cloud One

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

O Trend Micro Cloud One fornece as informações de segurança certas às equipes na hora e no local certos. Essa integração envia descobertas de segurança para o Security Hub em tempo real, aumentando a visibilidade de seus AWS recursos e detalhes do Trend Micro Cloud One evento no Security Hub.

AWS Link do Marketplace

Documentação do parceiro

Vectra – Cognito Detect

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

O Vectra está transformando a segurança cibernética aplicando IA avançada para detectar e responder a ataques cibernéticos ocultos antes que eles possam roubar ou causar danos.

AWS Link do Marketplace

Documentação do parceiro

Wiz – Wiz Security

Tipo de integração: envio

ARN do produto: `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wizanalisa continuamente configurações, vulnerabilidades, redes, configurações de IAM, segredos e muito mais em seus Contas da AWS usuários e cargas de trabalho para descobrir problemas críticos que representam riscos reais. Integre o Wiz com o Security Hub para visualizar e responder aos problemas que o Wiz detecta no console do Security Hub.

AWS Link do Marketplace

Documentação do parceiro

Integrações de terceiros que recebem descobertas do Security Hub

As seguintes integrações de produtos de parceiros terceirizados recebem descobertas do Security Hub. Onde indicado, os produtos também podem atualizar as descobertas. Nesse caso, descobrir atualizações feitas no produto parceiro também será refletido no Security Hub.

Atlassian - Jira Service Management

Tipo de integração: recebimento e atualização

O AWS Service Management Connector for Jira envia as descobertas do Security Hub paraJira. Jiraos problemas são criados com base nas descobertas. Quando os problemas no Jira são atualizados, as descobertas correspondentes são atualizadas no Security Hub.

A integração só é compatível com o Jira Server e o Jira Data Center.

Para uma visão geral da integração e de como ela funciona, assista ao vídeo AWS Security Hub – Integração bidirecional com o Atlassian Jira Service Management.

Link do produto

Documentação do parceiro

Atlassian - Jira Service Management Cloud

Tipo de integração: recebimento e atualização

O Jira Service Management Cloud é o componente de nuvem do Jira Service Management.

O AWS Service Management Connector for Jira envia as descobertas do Security Hub paraJira. As descobertas desencadeiam a criação de problemas no Jira Service Management Cloud. Quando você atualiza esses problemas na Jira Service Management Cloud, as descobertas correspondentes também são atualizadas no Security Hub.

Link do produto

Documentação do parceiro

Atlassian – Opsgenie

Tipo de integração: recebimento

A Opsgenieé uma solução moderna de gerenciamento de incidentes para operar serviços sempre ativos, capacitando as equipes de desenvolvimento e operações a planejar interrupções de serviço e permanecer no controle durante incidentes.

A integração com o Security Hub garante que os incidentes relacionados à segurança de missão crítica sejam direcionados para as equipes apropriadas para resolução imediata.

Link do produto

Documentação do parceiro

Fortinet – FortiCNP

Tipo de integração: recebimento

O FortiCNP é um produto do Cloud Native Protection que agrega descobertas de segurança em insights acionáveis e prioriza insights de segurança com base na pontuação de risco para reduzir a fadiga de alertas e acelerar a correção.

AWS Link do Marketplace

Documentação do parceiro

IBM – QRadar

Tipo de integração: recebimento

O IBM QRadar SIEM fornece às equipes de segurança a capacidade de detectar, priorizar, investigar e responder com rapidez e precisão às ameaças.

Link do produto

Documentação do parceiro

Logz.io Cloud SIEM

Tipo de integração: recebimento

O Logz.io é um fornecedor de Cloud SIEM que fornece correlação avançada de dados de log e eventos para ajudar as equipes de segurança a detectar, analisar e responder às ameaças à segurança em tempo real.

Link do produto

Documentação do parceiro

MetricStream – CyberGRC

Tipo de integração: recebimento

O MetricStream CyberGRC ajuda você a gerenciar, medir e mitigar os riscos de segurança cibernética. Ao receber as descobertas do Security Hub, o CyberGRC fornece mais visibilidade sobre esses riscos, para que você possa priorizar os investimentos em segurança cibernética e cumprir as políticas de TI.

AWS Link do Marketplace

Link do produto

MicroFocus – MicroFocus Arcsight

Tipo de integração: recebimento

O ArcSight acelera a detecção e a resposta eficazes a ameaças em tempo real, integrando correlação de eventos e análises supervisionadas e não supervisionadas com automação e orquestração de respostas.

Link do produto

Documentação do parceiro

New Relic Vulnerability Management

Tipo de integração: recebimento

O New Relic Vulnerability Management recebe descobertas de segurança do Security Hub, para que você possa ter uma visão centralizada da segurança juntamente com a telemetria de desempenho no contexto de toda a sua pilha.

AWS Link do Marketplace

Documentação do parceiro

PagerDuty – PagerDuty

Tipo de integração: recebimento

A plataforma de gerenciamento de operações digitais PagerDuty capacita as equipes a mitigar proativamente os problemas que afetam os clientes, transformando automaticamente qualquer sinal em um insight e uma ação corretas.

AWS os usuários podem usar o PagerDuty conjunto de AWS integrações para escalar seus ambientes AWS e ambientes híbridos com confiança.

Quando acoplado aos alertas de segurança agregados e organizados do Security Hub, o PagerDuty permite que as equipes automatizem o processo de resposta a ameaças e configurem rapidamente ações personalizadas para evitar possíveis problemas.

Os usuários do PagerDuty que executam um projeto de migração para a nuvem podem se mover rapidamente, enquanto diminuem o impacto de problemas que ocorrem durante todo o ciclo de vida da migração.

Link do produto

Documentação do parceiro

Palo Alto Networks – Cortex XSOAR

Tipo de integração: recebimento

O Cortex XSOAR é uma plataforma de Orquestração, Automação e Resposta de Segurança (SOAR) que se integra a toda a sua pilha de produtos de segurança para acelerar a resposta a incidentes e as operações de segurança.

Link do produto

Documentação do parceiro

Palo Alto Networks – VM-Series

Tipo de integração: recebimento

A integração do Palo Alto VM-Series com o Security Hub coleta informações sobre ameaças e as envia para o firewall de próxima geração do VM-Series como uma atualização automática da política de segurança que bloqueia atividades maliciosas de endereços IP.

Link do produto

Documentação do parceiro

Rackspace Technology – Cloud Native Security

Tipo de integração: recebimento

A Rackspace Technology fornece serviços de segurança gerenciados em cima de produtos de segurança nativos da AWS para monitoramento 24x7x365 do Rackspace SOC, análise avançada e correção de ameaças.

Link do produto

Rapid7 – InsightConnect

Tipo de integração: recebimento

O Rapid7 InsightConnect é uma solução de automação e orquestração de segurança que permite à sua equipe otimizar as operações do SOC com poucos códigos ou nenhum.

Link do produto

Documentação do parceiro

RSA – RSA Archer

Tipo de integração: recebimento

O gerenciamento de riscos de TI e segurança do RSA Archer permite que você determine quais ativos são essenciais para seus negócios, estabeleça e comunique políticas e padrões de segurança, detecte e responda a ataques, identifique e corrija deficiências de segurança e estabeleça as melhores práticas claras de gerenciamento de riscos de TI.

Link do produto

Documentação do parceiro

ServiceNow – ITSM

Tipo de integração: recebimento e atualização

A integração do ServiceNow com o Security Hub permite que você receba descobertas do Security Hub para serem visualizadas no ServiceNow ITSM. Você também pode configurar o ServiceNow para criar automaticamente um incidente ou problema ao receber uma descoberta do Security Hub.

Quaisquer atualizações desses incidentes e problemas resultarão em atualizações das descobertas no Security Hub.

Para uma visão geral da integração e de como ela funciona, assista ao vídeo AWS Security Hub - Integração bidirecional com ServiceNow ITSM.

Link do produto

Documentação do parceiro

Slack – Slack

Tipo de integração: recebimento

O Slack é uma camada da pilha de tecnologia de negócios que reúne pessoas, dados e aplicativos. Ele é um lugar único em que as pessoas podem efetivamente trabalhar juntas, encontrar informações importantes e acessar centenas de milhares de aplicativos e serviços essenciais para fazer o seu melhor trabalho.

Link do produto

Documentação do parceiro

Splunk – Splunk Enterprise

Tipo de integração: recebimento

Splunkusa a Amazon CloudWatch Events como consumidora das descobertas do Security Hub. Envie seus dados ao Splunk para análise de segurança avançada e SIEM.

Link do produto

Documentação do parceiro

Splunk – Splunk Phantom

Tipo de integração: recebimento

Com o Splunk Phantom aplicativo do AWS Security Hub, as descobertas são enviadas Phantom para enriquecimento automatizado do contexto com informações adicionais de inteligência sobre ameaças ou para realizar ações de resposta automatizadas.

Link do produto

Documentação do parceiro

ThreatModeler

Tipo de integração: recebimento

O ThreatModeler é uma solução automatizada de modelagem de ameaças que protege e dimensiona o ciclo de vida do desenvolvimento do software corporativo e da nuvem.

Link do produto

Documentação do parceiro

Trellix – Trellix Helix

Tipo de integração: recebimento

O Trellix Helix é uma plataforma de operações de segurança hospedada na nuvem que permite às organizações assumir o controle de qualquer incidente, desde o alerta até a correção.

Link do produto

Documentação do parceiro

Integrações de terceiros que enviam e recebem descobertas do Security Hub

As seguintes integrações de produtos de parceiros terceirizados enviam e recebem descobertas do Security Hub.

Caveonix – Caveonix Cloud

Tipo de integração: envio e recebimento

ARN do produto: `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

A plataforma Caveonix baseada em IA automatiza a visibilidade, a avaliação e a mitigação em nuvens híbridas, abrangendo serviços, VMs e contêineres nativos de nuvem. Integrado ao AWS Security Hub, Caveonix mescla AWS dados e análises avançadas para obter informações sobre alertas de segurança e conformidade.

AWS Link do Marketplace

Documentação do parceiro

Cloud Custodian – Cloud Custodian

Tipo de integração: envio e recebimento

ARN do produto: `arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

O Cloud Custodian permite que os usuários sejam bem gerenciados na nuvem. O YAML DSL simples permite regras facilmente definidas para habilitar uma infraestrutura de nuvem bem gerenciada que seja segura e otimizada para custos.

Link do produto

Documentação do parceiro

DisruptOps, Inc. – DisruptOPS

Tipo de integração: envio e recebimento

ARN do produto: `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

A DisruptOps Security Operations Platform (plataforma de operações de segurança) ajuda as organizações a manter as melhores práticas de segurança na nuvem por meio do uso de proteções automatizadas.

Link do produto

Documentação do parceiro

Kion

Tipo de integração: envio e recebimento

ARN do produto: `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion(anteriormente cloudtamer.io) é uma solução completa de governança em nuvem para. AWSKiondá às partes interessadas visibilidade das operações na nuvem e ajuda os usuários da nuvem a gerenciar contas, controlar o orçamento e os custos e garantir a conformidade contínua.

Link do produto

Documentação do parceiro

Turbot – Turbot

Tipo de integração: envio e recebimento

ARN do produto: `arn:aws:securityhub:<REGION>::product/turbot/turbot`

O Turbot garante que sua infraestrutura de nuvem seja segura, compatível, dimensionável e otimizada para custos.

Link do produto

Documentação do parceiro

Usando integrações personalizadas de produtos para enviar descobertas ao AWS Security Hub

Além das descobertas geradas pelos AWS serviços integrados e produtos de terceiros, o Security Hub pode consumir descobertas geradas por outros produtos de segurança personalizados.

Você pode enviar essas descobertas para o Security Hub manualmente usando a operação `BatchImportFindings`da API.

Ao configurar a integração personalizada, use as diretrizes e as listas de verificação fornecidas no Guia de integração de parceiros do Security Hub.

Requisitos e recomendações para enviar descobertas de produtos de segurança personalizados

Antes de invocar a operação de API `BatchImportFindings`, você deve habilitar o Security Hub.

Você deve fornecer os detalhes da descoberta usando o the section called “Formato de descoberta”. Para obter as descobertas de sua integração personalizada, use os seguintes requisitos e recomendações.

Configurar o ARN do produto

Quando você habilita o Security Hub, um nome do recurso da Amazon (ARN) do produto padrão para o Security Hub é gerado em sua conta atual.

Esse ARN do produto tem o seguinte formato: `arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default`. Por exemplo, `arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default`.

Use esse ARN do produto como o valor para o atributo `ProductArn` ao chamar a operação da API `BatchImportFindings`.

Definir o nome da empresa e do produto

Você pode usar o `BatchImportFindings` para definir um nome de empresa e um nome de produto preferidos para a integração personalizada que está enviando descobertas para o Security Hub.

Seus nomes especificados substituem o nome da empresa e o nome do produto pré-configurados, chamados de nome pessoal e nome padrão, respectivamente, e aparecem no console do Security Hub e no JSON de cada descoberta. Consulte Usar BatchImportFindings para criar e atualizar descobertas.

Definir os IDs de descoberta

Você deve fornecer, gerenciar e incrementar seus próprios IDs de descoberta, usando o atributo `Id`.

Cada nova descoberta deve ter um ID de descoberta exclusivo. Se o produto personalizado enviar várias descobertas com o mesmo ID de descoberta, o Security Hub processará somente a primeira descoberta.

Definir o ID da conta

Você deve especificar seu próprio ID de conta, usando o atributo `AwsAccountId`.

Definir as datas de criação e atualização

Você deve fornecer seus próprios carimbos de data/hora para os atributos `CreatedAt` e `UpdatedAt`.

Atualizar descobertas de produtos personalizados

Além de enviar novas descobertas de produtos personalizados, também é possível usar a operação de API `BatchImportFindings` para atualizar descobertas existentes de produtos personalizados.

Para atualizar descobertas existentes, use o ID da descoberta existente (pelo atributo `Id`). Reenvie a descoberta completa com as informações apropriadas atualizadas na solicitação, incluindo um time stamp `UpdatedAt` modificado.

Integrações personalizadas de exemplo

Você pode usar as integrações personalizadas de produtos a seguir como um guia para criar sua própria solução personalizada.

Enviando descobertas de verificações do Chef InSpec para o Security Hub

Você pode criar um AWS CloudFormation modelo que executa uma verificação de Chef InSpec conformidade e, em seguida, envia as descobertas para o Security Hub.

Para mais detalhes, consulte o Monitoramento contínuo de conformidade com o Chef InSpec e o AWS Security Hub.

Enviando vulnerabilidades de contêiner detectadas pelo Trivy ao Security Hub

Você pode criar um AWS CloudFormation modelo usado AquaSecurity Trivy para escanear contêineres em busca de vulnerabilidades e, em seguida, enviar essas descobertas de vulnerabilidade para o Security Hub.

Para obter mais detalhes, consulte Como criar um pipeline de CI/CD para verificação de vulnerabilidades de contêineres com o AWS Security Trivy Hub.

Controles e padrões de AWS segurança no Security Hub

AWS O Security Hub consome, agrega e analisa as descobertas de segurança de vários produtos compatíveis AWS e de terceiros.

O Security Hub também gera suas próprias descobertas executando verificações de segurança automatizadas e contínuas de acordo com as regras. As regras são representadas por controles de segurança. Os controles podem, por sua vez, ser habilitados em um ou mais padrões de segurança. Os controles ajudam a determinar se os requisitos de um padrão estão sendo atendidos.

As verificações de segurança em relação aos controles geram descobertas que você pode usar para monitorar sua postura de segurança e identificar recursos específicos Contas da AWS ou que requerem atenção. Cada controle está relacionado a um AWS serviço e recurso. Por exemplo, as verificações de segurança do controle CloudTrail.4 determinam se você configurou a validação do arquivo de log em seus AWS CloudTrail registros. Para obter mais informações sobre tabelas de controle, consulte Visualizando e gerenciando padrões de segurança.

É possível habilitar um controle em um ou mais padrões habilitados do Security Hub. Quando você ativa um padrão, o Security Hub ativa automaticamente os controles que se aplicam ao padrão. Os padrões de segurança permitem que você se concentre em uma estrutura de conformidade específica. O Security Hub define os controles que se aplicam a cada padrão. Para obter mais informações sobre grupos de segurança, consulte e .

Com base nos resultados das verificações de segurança, o Security Hub calcula uma pontuação geral de segurança e pontuações de segurança específicas do padrão. Essas pontuações ajudam você a entender sua postura de segurança. Para obter mais informações sobre escopos, consulte Como as pontuações de segurança são calculadas.

Para mais informações sobre como o Security Hub cobra por descobertas de ingestão e verificações de segurança, consulte a Definição de preços do Security Hub.

Tópicos

- Visualizando e gerenciando padrões de segurança

Permissões do IAM para configurar padrões e controles

Para visualizar informações sobre controles de segurança e habilitar e desabilitar controles de segurança em padrões, a função AWS Identity and Access Management (IAM) que você usa para acessar AWS Security Hub precisa de permissões para chamar as seguintes ações de API. Sem adicionar permissões para essas ações, você não poderá chamar essas APIs. Para obter as permissões necessárias, é possível usar as políticas gerenciadas do Security Hub. Como alternativa, é possível atualizar as políticas de IAM personalizadas para incluir essas ações. As políticas personalizadas também devem incluir permissões para as APIs `UpdateStandardsControl` e `DescribeStandardsControls`.

- **`BatchGetSecurityControls`**— Retorna informações sobre um lote de controles de segurança para a conta corrente Região da AWS e.
- **`ListSecurityControlDefinitions`** — Retorna informações sobre controles de segurança que se aplicam a um padrão específico.
- **`ListStandardsControlAssociations`** — Identifica se um controle de segurança está atualmente ativado ou desativado em cada padrão ativado na conta.
- **`BatchGetStandardsControlAssociations`** — Para um lote de controles de segurança, identifica se cada controle está atualmente ativado ou desativado a partir de um padrão especificado.
- **`BatchUpdateStandardsControlAssociations`** — Usado para ativar um controle de segurança em padrões que incluem o controle ou para desativar um controle em padrões. Esse é um substituto em lote da API `UpdateStandardsControl` existente se um administrador não quiser permitir que as contas dos membros ativem ou desativem os controles.

Além das APIs anteriores, você deve adicionar permissão para chamar **`BatchGetControlEvaluations`** para seu perfil do IAM. Concede permissão para obter o status de habilitação e conformidade dos controles, a contagem de descobertas para os controles e a pontuação geral de segurança dos controles no console do Security Hub Como somente o console chama **`BatchGetControlEvaluations`**, essa permissão do IAM não corresponde diretamente às APIs ou AWS CLI comandos do Security Hub documentados publicamente.

Para obter mais informações sobre APIs relacionadas a controles e padrões, consulte Referência da API AWS Security Hub.

Verificações de segurança e pontuações de segurança no Security Hub

Para cada controle que você habilita, AWS Security Hub executa verificações de segurança. Uma verificação de segurança determina se seus AWS recursos estão em conformidade com as regras que o controle inclui.

Algumas verificações são executadas em uma programação periódica. Outras verificações são executadas somente quando há uma alteração no estado do recurso. Para ter mais informações, consulte the section called “Programar a execução de verificações de segurança”.

Muitas verificações de segurança usam regras AWS Config gerenciadas ou personalizadas para estabelecer os requisitos de conformidade. Para executar essas verificações, você deve configurar AWS Config. Para ter mais informações, consulte the section called “AWS Config regras e verificações de segurança”. Outros usam funções do Lambda personalizadas, que são gerenciadas pelo Security Hub e não são visíveis para os clientes.

À medida que o Security Hub executa verificações de segurança, ele gera descobertas e atribui a elas um status de conformidade. Para obter mais informações sobre conformidade, consulte Valores do status de conformidade de uma descoberta.

O Security Hub usa o status de conformidade das descobertas de controle para determinar um status geral de controle. O Security Hub também calcula uma pontuação de segurança em todos os controles habilitados e para padrões específicos. Para obter mais informações, consulte the section called “Status de conformidade e status de controle” e the section called “Determinando as pontuações de segurança”.

Se você ativou as descobertas de controle consolidadas, o Security Hub gera uma única descoberta mesmo quando um controle está associado a mais de um padrão. Para ter mais informações, consulte Ativar/desativar descobertas de controle consolidadas.

Tópicos

- Determinando as pontuações de segurança

Como o Security Hub usa AWS Config regras para executar verificações de segurança

Para executar verificações de segurança nos recursos do seu ambiente, AWS Security Hub use etapas especificadas pelo padrão ou use AWS Config regras específicas. Algumas regras são regras gerenciadas, que são gerenciadas por AWS Config. Outras regras são regras personalizadas que o Security Hub desenvolve.

AWS Config as regras que o Security Hub usa para controles são chamadas de regras vinculadas ao serviço, porque são habilitadas e controladas pelo serviço do Security Hub.

Para habilitar a verificação dessas AWS Config regras, você deve primeiro ativar AWS Config sua conta e ativar o registro de recursos para os recursos necessários. Para obter informações sobre como habilitar AWS Config, consulteConfigurando AWS Config. Para obter mais informações sobre conjuntos de registros de recursos, consulte AWS Config recursos necessários para gerar resultados de controle.

Como o gera regras vinculadas ao serviço do para padrões de segurança

Para cada controle que usa uma regra AWS Config vinculada ao serviço, o Security Hub cria instâncias das regras necessárias em seu AWS ambiente.

Essas regras vinculadas ao serviço são específicas do . Ele cria essas regras vinculadas ao serviço mesmo se outras instâncias das mesmas regras já existirem. A regra vinculada ao serviço adiciona `securityhub` antes do nome da regra original e um identificador exclusivo após o nome da regra. Por exemplo, para a regra AWS Config gerenciada original`vpc-flow-logs-enabled`, o nome da regra vinculada ao serviço seria algo como. `securityhub-vpc-flow-logs-enabled-12345`

Há limites no número de AWS Config regras que podem ser usadas para avaliar os controles. AWS Config As regras personalizadas criadas pelo Security Hub não contam para esse limite. Você pode ativar um padrão de segurança mesmo que já tenha atingido o AWS Config limite de regras gerenciadas em sua conta. Para saber mais sobre os limites das AWS Config regras, consulte Limites de serviço no Guia do AWS Config desenvolvedor.

Visualizando detalhes sobre as regras AWS Config para controles

Para controles que usam regras AWS Config gerenciadas, a descrição do controle inclui um link para os detalhes da AWS Config regra. As regras personalizadas não estão vinculadas à descrição do controle. Para obter descrições de controle, consulte Referência de controles do Security Hub. Selecione um controle na lista para ver sua descrição.

Para descobertas geradas a partir desses controles, os detalhes da descoberta incluem um link para a AWS Config regra associada. Observe que, para acessar a AWS Config regra a partir da busca de detalhes, você também precisa ter uma permissão do IAM na conta selecionada para acessar AWS Config.

Os detalhes da descoberta na página Descobertas, na página Insights e na página Integrações incluem um link de Regras para os detalhes da regra AWS Config . Consulte Analisando os detalhes da descoberta.

Na página de detalhes do controle, a coluna Investigar da lista de descobertas contém um link para os detalhes da AWS Config regra. Consulte Visualizando a AWS Config regra para um recurso de busca.

AWS Config recursos necessários para gerar resultados de controle

AWS Security Hub gera descobertas de controle executando verificações de segurança em relação aos controles do Security Hub. Alguns controles usam AWS Config regras que avaliam a conformidade com recursos específicos. Para que o Security Hub gere descobertas para controles que tenham um tipo de programação acionado por alteração, você deve ativar a gravação dos recursos necessários em AWS Config. Você não precisa registrar recursos para a maioria dos controles que têm um tipo de programação periódico. Entretanto, alguns controles periódicos exigem o registro de recursos para detectar alterações na conformidade.

Esta página fornece uma lista dos recursos necessários em todos os padrões e uma lista dos recursos necessários divididos por padrão. A primeira tabela também lista quais controles do Security Hub usam cada recurso.

Se uma descoberta for gerada por uma verificação de segurança baseada em uma AWS Config regra, os detalhes da descoberta incluirão um link de Regras para a AWS Config regra associada. Para navegar até a AWS Config regra, sua conta precisa ter permissões do IAM para visualizar AWS Config as regras.

> **Note**
>
> Regiões da AWS Quando um controle não está disponível, o recurso correspondente não está disponível em AWS Config. Para obter uma lista dos limites regionais nos controles do Security Hub, consulte Disponibilidade de controles por região.

AWS Config recursos necessários para todos os controles

Para que o Security Hub gere descobertas para controles ativados por alterações do Security Hub que usam uma AWS Config regra, você deve registrar esses recursos em AWS Config. Essa tabela também indica quais controles exigem um recurso específico. Um controle pode exigir mais do que um recurso.

Serviço	Recursos necessários do	Controles relacionados
Amazon API Gateway	`AWS::ApiGateway::Stage`	APIGateway.1 APIGateway.1 APIGateway.1 APIGateway.1 APIGateway.1
	`AWS::ApiGatewayV2::Stage`	APIGateway.1 APIGateway.1
AWS AppSync	`AWS::AppSync::GraphQLApi`	AppSync.2 AppSync.4 AppSync5.
AWS Backup (AWS Backup)	`AWS::Backup::RecoveryPoint`	Backup.1

Serviço	Recursos necessários do	Controles relacionados
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`	ACM.1 ACM.1 CM3
Amazon Athena	`AWS::Athena::DataCatalog`	Atena.2
	`AWS::Athena::WorkGroup`	`Athena.3`
AWS CloudFormation	`AWS::CloudFormation::Stack`	CloudFormation.1 CloudFormation.2
Amazon CloudFront	`AWS::CloudFront::Distribution`	CloudFront.1 CloudFront.3 CloudFront.4 CloudFront5. CloudFront.6 CloudFront7. CloudFront8. CloudFront9. CloudFront.10 CloudFront1.3 CloudFront1.4

Serviço	Recursos necessários do	Controles relacionados
AWS CloudTrail	`AWS::CloudTrail::Trail`	CloudTrail9.
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	CloudWatch1.5 CloudWatch1.7
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	CodeArtifact.1
AWS CodeBuild	`AWS::CodeBuild::Project`	CodeBuild.1 CodeBuild.2 CodeBuild.3 CodeBuild.4
Amazon Detective	`AWS::Detective::Graph`	Detetive.1
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Certificate`	DMS.2

	`AWS::DMS::Endpoint`	`DMS.9`
		`DMS.10`
		`DMS.11`
		`DMS.12`

	`AWS::DMS::EventSubscription`	DMS. 3

Serviço	Recursos necessários do	Controles relacionados
	`AWS::DMS::ReplicationInstance`	DMS. 4 DMS.1
	`AWS::DMS::ReplicationSubnetGroup`	DMS. 5
	`AWS::DMS::ReplicationTask`	DMS.1 DMS.1
Amazon DynamoDB	`AWS::DynamoDB::Table`	DynamoDB.2 DynamoDB.6
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`	EC2.51
	`AWS::EC2::CustomerGateway`	EC2.36
	`AWS::EC2::EIP`	EC2.12 EC2.37
	`AWS::EC2::FlowLog`	EC2.48

Serviço	Recursos necessários do	Controles relacionados
	`AWS::EC2::Instance`	EC2.4 EC2.8 EC2.9 EC2.17 EC2.24 EC2.38 EMR.1 SSM.3
	`AWS::EC2::InternetGateway`	EC2.39
	`AWS::EC2::LaunchTemplate`	EC2.25
	`AWS::EC2::NatGateway`	EC2.40
	`AWS::EC2::NetworkAcl`	EC2.16 EC2.21 EC2.41
	`AWS::EC2::NetworkInterface`	EC2.22 EC2.35

Serviço	Recursos necessários do	Controles relacionados
	`AWS::EC2::RouteTable`	EC2.42
	`AWS::EC2::SecurityGroup`	EC2.2 EC2.13 EC2.14 EC2.18 EC2.19 EC2.43
	`AWS::EC2::Subnet`	EC2.15 EC2.44 ElastiCache7. Lambda.5
	`AWS::EC2::TransitGateway`	EC2.23 EC2.52
	`AWS::EC2::TransitGatewayAttachment`	EC2.33
	`AWS::EC2::TransitGatewayRouteTable`	EC2.34

Serviço	Recursos necessários do	Controles relacionados
	`AWS::EC2::Volume`	EC2.3 EC2.45
	`AWS::EC2::VPC`	EC2.46
	`AWS::EC2::VPCEndpointService`	EC2.47
	`AWS::EC2::VPCPeeringConnector`	EC2.49
	`AWS::EC2::VPNConnection`	EC2.20
	`AWS::EC2::VPNGateway`	EC2.50
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	AutoScaling.1 AutoScaling.2 AutoScaling.6 AutoScaling9. AutoScaling.10
	`AWS::AutoScaling::LaunchConfiguration`	AutoScaling.3 Auto Scaling

Serviço	Recursos necessários do	Controles relacionados
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`	SSM.3
	`AWS::SSM::ManagedInstanceInventory`	SSM.1
	`AWS::SSM::PatchCompliance`	SSM.3
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`	ECR.4
	`AWS::ECR::Repository`	ECR.2 ECR.2
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`	ECS.12 ECS.14
	`AWS::ECS::Service`	ECS.12 ECS.12 ECS.13

Serviço	Recursos necessários do	Controles relacionados
	`AWS::ECS::TaskDefinition`	ECS.12 ECS.12 ECS.12 ECS.12 ECS.12 ECS.12 ECS.15
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`	EFS.3 EFS.3 EFS.5
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`	eks.2 POR EXEMPLO. 6
	`AWS::EKS::IdentityProviderConfig`	POR EXEMPLO. 7
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`	ElasticBeanstalk.1 ElasticBeanstalk.2 ElasticBeanstalk.3

Serviço	Recursos necessários do	Controles relacionados
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`	ELB.1 ELB.1 ELB.1 ELB.1 ELB.1 ELB.1 ELB.1 ELB.1
	`AWS::ElasticLoadBalancingV2::LoadBalancer`	ELB.1 ELB.1 ELB.1 ELB.1 ELB.1 ELB.1

Serviço	Recursos necessários do	Controles relacionados
ElasticSearch	`AWS::Elasticsearch::Domain`	ES.1 ES.1 ES.1 ES.1 ES.1 ES.1 ES.9
Amazon EventBridge	`AWS::Events::EventBus`	EventBridge.2 EventBridge.3
	`AWS::Events::Endpoint`	EventBridge.4
`Amazon FSx`	`AWS::FSx::FileSystem`	FSx.1
`AWS Global Accelerator`	`AWS::GlobalAccelerator::Accelerator`	GlobalAccelerator.1
`AWS Glue`	`AWS::Glue::Job`	Cola.1
`Amazon GuardDuty`	`AWS::GuardDuty::Detector`	GuardDuty.4
	`AWS::GuardDuty::Filter`	GuardDuty.2

Serviço	Recursos necessários do	Controles relacionados
	`AWS::GuardDuty::IPSet`	GuardDuty.3
AWS Identity and Access Management (IAM)	`AWS::IAM::Group`	IAM.18 EU SOU 27 KMS.2
	`AWS::IAM::Policy`	IAM.2 IAM.15 KMS.4
	`AWS::IAM::Role`	IAM.15 EU SOU 24 EU SOU 27 KMS.4
	`AWS::IAM::User`	IAM.2 IAM.18 EU SOU 25 EU SOU 27 KMS.2
AWS Identity and Access Management Access Analyzer	`AWS::AccessAnalyzer::Analyzer`	EU SOU 23
AWS IoT	`AWS::IoT::Authorizer`	IoT.4

Serviço	Recursos necessários do	Controles relacionados
	`AWS::IoT::Dimension`	IoT.3
	`AWS::IoT::MitigationAction`	IoT.2
	`AWS::IoT::Policy`	IoT.6
	`AWS::IoT::RoleAlias`	IoT.5
	`AWS::IoT::SecurityProfile`	IoT.1
AWS Key Management Service (AWS KMS)	`AWS::KMS::Key`	KMS.4
Amazon Kinesis	`AWS::Kinesis::Stream`	Kinesis.1 Cinesia.2
AWS Lambda	`AWS::Lambda::Function`	Lambda.1 Lambda.1 Lambda.1 Lambda.5 Lambda.6

Serviço	Recursos necessários do	Controles relacionados
Amazon MSK	`AWS::MSK::Cluster`	MSK.1 MSK.2
Amazon MQ	`AWS::AmazonMQ::Broker`	MQ.2 MQ.3 MQ.4 MQ.5 MQ.5
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	NetworkFirewall.1 NetworkFirewall7. NetworkFirewall9.
	`AWS::NetworkFirewall::FirewallPolicy`	NetworkFirewall.3 NetworkFirewall.4 NetworkFirewall5. NetworkFirewall8.
	`AWS::NetworkFirewall::RuleGroup`	NetworkFirewall.6

Serviço	Recursos necessários do	Controles relacionados
OpenSearch Serviço Amazon	`AWS::OpenSearch::Domain`	OpenSearch 1.3 OpenSearch 1.3 OpenSearch 1.3 OpenSearch 1.3 OpenSearch 1.3 OpenSearch 1.3 OpenSearch 1.3 OpenSearch 1.3 Pesquisa aberta. 9 Opensearch.10 Abrir pesquisa. 11

Serviço	Recursos necessários do	Controles relacionados
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`	DocumentDB DocumentDB DocumentDB DocumentDB Neptune.1 Neptune.1 Neptune.1 Neptune.1 Neptune.1 Neptune.1 Neptune.9 RDS. 3 RDS. 3 RDS. 3 RDS. 3 RDS. 3 RDS. 3 RDS. 3 RDS. 3 RDS.28 RDS. 3

Serviço	Recursos necessários do	Controles relacionados
		RDS. 3
	`AWS::RDS::DBClusterSnapshot`	DocumentDB Neptune.3 Neptune.3 RDS. 3 RDS. 3 RDS.29

Serviço	Recursos necessários do	Controles relacionados
	`AWS::RDS::DBInstance`	RDS. 3 RDS. 3 RDS. 3 RDS. 3 RDS. 3 RDS. 3 RDS. 3 RDS. 3 RDS. 3 RDS. 3 RDS. 3 RDS. 3 RDS. 3 RDS.30
	`AWS::RDS::DBSecurityGroup`	RDS.31
	`AWS::RDS::DBSnapshot`	DocumentDB RDS. 3 RDS. 3 RDS.32

Serviço	Recursos necessários do	Controles relacionados
	`AWS::RDS::DBSubnetGroup`	RDS.33
	`AWS::RDS::EventSubscription`	RDS. 3 RDS. 3 RDS. 3 RDS. 3
Amazon Redshift	`AWS::Redshift::Cluster`	5439 (Redshift) 5439 (Redshift) 5439 (Redshift) Redshift.4 Redshift.4 Redshift.4 Redshift.4 Redshift.9 Redshift.9 Desvio para o vermelho.11
	`AWS::Redshift::ClusterParameterGroup`	Redshift.2

Serviço	Recursos necessários do	Controles relacionados
	`AWS::Redshift::ClusterSnapshot`	Desvio para o vermelho.13
	`AWS::Redshift::ClusterSubnetGroup`	Desvio para o vermelho.14
	`AWS::Redshift::EventSubscription`	Desvio para o vermelho.12
Amazon Route 53	`AWS::Route53::HostedZone`	Route53.2
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint`	S3.19

Serviço	Recursos necessários do	Controles relacionados
	`AWS::S3::Bucket`	S3.2 S3.3 S3.5 S3.6 S3.7 S3.8 S3.9 S3.10 S3.11 S3.12 S3.13 S3.14 S3.15 S3.17 S3.20
AWS Secrets Manager	`AWS::SecretsManager::Secret`	SecretsManager.1 SecretsManager.2 SecretsManager5.
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`	ServiceCatalog.1

Serviço	Recursos necessários do	Controles relacionados
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet`	SEX.2
	`AWS::SES::ContactList`	SEX.1
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`	SNS.1 SNS.3
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`	SQS.1 SQ.2
Amazon SageMaker	`AWS::SageMaker::NotebookInstance`	SageMaker.2 SageMaker.3
AWS Step Functions	`AWS::StepFunctions::StateMachine`	StepFunctions.1 StepFunctions.2
AWS Transfer Family	`AWS::Transfer::Workflow`	Transferência.1
AWS WAF	`AWS::WAF::Rule`	WAF.6
	`AWS::WAF::RuleGroup`	WAF.6
	`AWS::WAF::WebACL`	WAF.6
	`AWS::WAFRegional::Rule`	WAF.6

Serviço	Recursos necessários do	Controles relacionados
	`AWS::WAFRegional::RuleGroup`	WAF.6
	`AWS::WAFRegional::WebACL`	WAF.6
	`AWS::WAFv2::RuleGroup`	WAF.6
	`AWS::WAFv2::WebACL`	WAF.6

Recursos necessários para o padrão FSBP

Para que o Security Hub relate com precisão as descobertas dos controles acionados por alterações ativadas pelas melhores práticas de segurança AWS básicas (FSBP) habilitados que usam uma AWS Config regra, você deve registrar esses recursos em. AWS Config Para obter mais informações sobre essa declaração de política, consulte AWS Padrão Foundational Security Best Practices (FSBP).

Serviço	Recursos necessários do
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`

Serviço	Recursos necessários do
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CodeBuild	`AWS::CodeBuild::Project`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint`
	`AWS::DMS::ReplicationInstance`
	`AWS::DMS::ReplicationTask`

Amazon DynamoDB	`AWS::DynamoDB::Table`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`
	`AWS::EC2::Instance`
	`AWS::EC2::LaunchTemplate`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::TransitGateway`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

Serviço	Recursos necessários do
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`

Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon EKS	`AWS::EKS::Cluster`
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon FSx	`AWS::FSx::FileSystem`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

Serviço	Recursos necessários do
AWS Key Management Service (AWS KMS)	`AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MSK	`AWS::MSK::Cluster`

AWS Network Firewall	`AWS::NetworkFirewall::Firewall`
	`AWS::NetworkFirewall::FirewallPolicy`
	`AWS::NetworkFirewall::RuleGroup`

OpenSearch Serviço Amazon	`AWS::OpenSearch::Domain`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint` `AWS::S3::Bucket`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`

Serviço	Recursos necessários do
Amazon SageMaker	`AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Step Functions	`AWS::StepFunctions::StateMachine`

AWS WAF	`AWS::WAF::Rule`
	`AWS::WAF::RuleGroup`
	`AWS::WAF::WebACL`
	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::RuleGroup`
	`AWS::WAFv2::WebACL`

Recursos necessários para o CIS AWS Foundations Benchmark

Para executar verificações de segurança de controles habilitados que se aplicam ao benchmark de AWS fundamentos do Center for Internet Security (CIS), o Security Hub executa as etapas de auditoria exatas prescritas para as verificações em Protegendo a Amazon Web Services ou usa regras gerenciadas específicas AWS Config .

Para obter mais informações sobre essa declaração de política, consulte Referências do CIS AWS Foundations.

Recursos necessários para o CIS v3.0.0

Para que o Security Hub relate com precisão as descobertas dos controles acionados por alterações habilitados do CIS v3.0.0 que usam uma AWS Config regra, você deve registrar esses recursos em. AWS Config

Serviço	Recursos necessários do

Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::Instance`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::SecurityGroup`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::User`
	`AWS::IAM::Role`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

Recursos necessários para o CIS v1.4.0

Para que o Security Hub relate com precisão as descobertas dos controles acionados por alterações habilitados do CIS v1.4.0 que usam uma AWS Config regra, você deve registrar esses recursos em. AWS Config

Serviço	Recursos necessários do
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::NetworkAcl` `AWS::EC2::SecurityGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` `AWS::IAM::User`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

Recursos necessários para o CIS v1.4.0

Para que o Security Hub relate com precisão as descobertas dos controles ativados por alterações do CIS v1.2.0 habilitados que usam uma AWS Config regra, você deve registrar esses recursos em. AWS Config

Serviço	Recursos necessários do
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::SecurityGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` `AWS::IAM::User`

Recursos necessários para o NIST SP 800-53 Rev. 5

Para que o Security Hub relate com precisão as descobertas dos controles acionados por alterações habilitados do National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 que usam uma AWS Config regra, você deve registrar esses recursos em. AWS Config Você só precisa registrar recursos para controles que tenham um tipo de programação acionado por alterações. Para obter mais informações sobre essa declaração de política, consulte Instituto Nacional de Padrões e Tecnologia (National Institute of Standards and Technology, NIST) SP 800-53 (Revisão 4).

Serviço	Recursos necessários do
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`

Serviço	Recursos necessários do
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
AWS CodeBuild	`AWS::CodeBuild::Project`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint`
	`AWS::DMS::ReplicationInstance`
	`AWS::DMS::ReplicationTask`

Amazon DynamoDB	`AWS::DynamoDB::Table`

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`
	`AWS::EC2::EIP`
	`AWS::EC2::Instance`
	`AWS::EC2::LaunchTemplate`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::TransitGateway`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`

Serviço	Recursos necessários do
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`

Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon EKS	`AWS::EKS::Cluster`
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EventBridge	`AWS::Events::Endpoint` `AWS::Events::EventBus`
Amazon FSx	`AWS::FSx::FileSystem`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Key`

Serviço	Recursos necessários do
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MSK	`AWS::MSK::Cluster`
Amazon MQ	`AWS::AmazonMQ::Broker`

AWS Network Firewall	`AWS::NetworkFirewall::Firewall`
	`AWS::NetworkFirewall::FirewallPolicy`
	`AWS::NetworkFirewall::RuleGroup`

OpenSearch Serviço Amazon	`AWS::OpenSearch::Domain`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint` `AWS::S3::Bucket`
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`

Serviço	Recursos necessários do
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

Amazon SageMaker	`AWS::SageMaker::NotebookInstance`
AWS Secrets Manager	`AWS::SecretsManager::Secret`

AWS WAF	`AWS::WAF::Rule`
	`AWS::WAF::RuleGroup`
	`AWS::WAF::WebACL`
	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::RuleGroup`
	`AWS::WAFv2::WebACL`

Recursos necessários para o PCI DSS v3.2.1

Para que o Security Hub relate com precisão as descobertas dos controles do Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) habilitados que usam uma AWS Config regra, você deve registrar esses recursos em. AWS Config Para obter mais informações sobre essa declaração de política, consulte Padrão de segurança de dados do setor de cartão de pagamento (PCI DSS – Payment Card Industry Data Security Standard).

Serviço	Recursos necessários do
AWS CodeBuild	`AWS::CodeBuild::Project`

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::EIP`
	`AWS::EC2::Instance`
	`AWS::EC2::SecurityGroup`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
AWS Identity and Access Management (IAM)	`AWS::IAM::Policy` `AWS::IAM::User`
AWS Lambda	`AWS::Lambda::Function`
OpenSearch Serviço Amazon	`AWS::OpenSearch::Domain`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`

Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

Recursos necessários para o AWS Resource Tagging Standard

Todos os controles no AWS Resource Tagging Standard são acionados por alterações e usam uma AWS Config regra. Para que o Security Hub relate com precisão as descobertas desses controles, você deve registrar os seguintes recursos em AWS Config. Você só precisa registrar recursos para controles que tenham um tipo de programação acionado por alterações. Para obter mais informações sobre essa declaração de política, consulte AWS Padrão de marcação de recursos.

Serviço	Recursos necessários do
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS AppSync	`AWS::AppSync::GraphQLApi`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
Amazon Athena	`AWS::Athena::DataCatalog` `AWS::Athena::WorkGroup`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CloudTrail	`AWS::CloudTrail::Trail`
AWS CodeArtifact	`AWS::CodeArtifact::Repository`
Amazon Detective	`AWS::Detective::Graph`

AWS Database Migration Service (AWS DMS)	`AWS::DMS::Certificate`
	`AWS::DMS::EventSubscription`
	`AWS::DMS::ReplicationInstance`
	`AWS::DMS::ReplicationSubnetGroup`

Serviço	Recursos necessários do
Amazon DynamoDB	`AWS::DynamoDB::Trail`

Serviço	Recursos necessários do

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::CustomerGateway`
	`AWS::EC2::EIP`
	`AWS::EC2::FlowLog`
	`AWS::EC2::Instance`
	`AWS::EC2::InternetGateway`
	`AWS::EC2::NatGateway`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::RouteTable`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::TransitGateway`
	`AWS::EC2::TransitGatewayAttachment`
	`AWS::EC2::TransitGatewayRouteTable`
	`AWS::EC2::Volume`
	`AWS::EC2::VPC`
	`AWS::EC2::VPCEndpointService`
	`AWS::EC2::VPCPeeringConnector`
	`AWS::EC2::VPNGateway`

Serviço	Recursos necessários do
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`

Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster` `AWS::EKS::IdentityProviderConfig`
AWS Elastic Beanstalk (Elastic Beanstalk)	`AWS::ElasticBeanstalk::Environment`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EventBridge	`AWS::Events::EventBus`
AWS Global Accelerator	`AWS::GlobalAccelerator::Accelerator`
AWS Glue	`AWS::Glue::Job`

Amazon GuardDuty	`AWS::GuardDuty::Detector`
	`AWS::GuardDuty::Filter`
	`AWS::GuardDuty::IPSet`

AWS Identity and Access Management (IAM)	`AWS::IAM::Role` `AWS::IAM::User`
AWS Identity and Access Management Access Analyzer (Analisador de acesso IAM)	`AWS::AccessAnalyzer::Analyzer`

Serviço	Recursos necessários do

AWS IoT	`AWS::IoT::Authorizer`
	`AWS::IoT::Dimension`
	`AWS::IoT::MitigationAction`
	`AWS::IoT::Policy`
	`AWS::IoT::RoleAlias`
	`AWS::IoT::SecurityProfile`

Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` `AWS::NetworkFirewall::Firew allPolicy`
OpenSearch Serviço Amazon	`AWS::OpenSearch::Domain`

Amazon Relational Database Service	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSecurityGroup`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::DBSubnetGroup`

Serviço	Recursos necessários do

Amazon Redshift	`AWS::Redshift::Cluster`
	`AWS::Redshift::ClusterSnapshot`
	`AWS::Redshift::ClusterSubnetGroup`
	`AWS::Redshift::EventSubscription`

AWS Secrets Manager	`AWS::SecretsManager::Secret`
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet` `AWS::SES::ContactList`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
AWS Step Functions	`AWS::StepFunctions::Activity`
AWS Transfer Family	`AWS::Transfer::Workflow`

Recursos necessários para o Service-Managed Standard: AWS Control Tower

Para que o Security Hub relate com precisão as descobertas do Padrão Gerenciado por Serviços habilitado: AWS Control Tower altere os controles acionados que usam uma AWS Config regra, você deve registrar os seguintes recursos em. AWS Config Para obter mais informações sobre essa declaração de política, consulte Padrão gerenciado por serviços: AWS Control Tower.

Serviço	Recursos necessários do
Amazon API Gateway	`AWS::ApiGateway::Stage` `AWS::ApiGatewayV2::Stage`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`

Serviço	Recursos necessários do
AWS CodeBuild	`AWS::CodeBuild::Project`
Amazon DynamoDB	`AWS::DynamoDB::Table`

Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::Instance`
	`AWS::EC2::NetworkAcl`
	`AWS::EC2::NetworkInterface`
	`AWS::EC2::SecurityGroup`
	`AWS::EC2::Subnet`
	`AWS::EC2::VPNConnection`
	`AWS::EC2::Volume`

Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`

Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`
	`AWS::ECS::Service`
	`AWS::ECS::TaskDefinition`

Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon EKS	`AWS::EKS::Cluster`
ElasticBeanstalk	`AWS::ElasticBeanstalk::Environment`

Serviço	Recursos necessários do
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`

AWS Identity and Access Management (IAM)	`AWS::IAM::Group`
	`AWS::IAM::Policy`
	`AWS::IAM::Role`
	`AWS::IAM::User`

AWS Key Management Service (AWS KMS)	`AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` `AWS::NetworkFirewall::RuleGroup`
OpenSearch Serviço Amazon	`AWS::OpenSearch::Domain`

Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`
	`AWS::RDS::DBClusterSnapshot`
	`AWS::RDS::DBInstance`
	`AWS::RDS::DBSnapshot`
	`AWS::RDS::EventSubscription`

Amazon Redshift	`AWS::Redshift::Cluster`

Serviço	Recursos necessários do
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`

Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`
	`AWS::SSM::ManagedInstanceInventory`
	`AWS::SSM::PatchCompliance`

AWS Secrets Manager	`AWS::SecretsManager::Secret`

AWS WAF	`AWS::WAFRegional::Rule`
	`AWS::WAFRegional::RuleGroup`
	`AWS::WAFRegional::WebACL`
	`AWS::WAFv2::WebACL`

Programar a execução de verificações de segurança

Depois de habilitar um padrão de segurança, AWS Security Hub começa a executar todas as verificações em duas horas. A maioria das verificações começa a ser executada em 25 minutos. O Security Hub executa verificações avaliando a regra subjacente a um controle. Até que um controle conclua sua primeira execução de verificações, seu status é Sem dados.

Quando você habilita um novo padrão, o Security Hub pode levar até 24 horas para gerar descobertas para controles que usam a mesma regra subjacente AWS Config vinculada ao serviço dos controles habilitados de outros padrões habilitados. Por exemplo, se você habilitar o Lambda.1 no padrão AWS Foundational Security Best Practices (FSBP), o Security Hub criará a regra vinculada ao serviço e normalmente gerará descobertas em minutos. Depois disso, se você habilitar o Lambda.1 no Payment Card Industry Data Security Standard (PCI DSS), o Security Hub poderá

levar até 24 horas para gerar descobertas para esse controle, pois ele usa a mesma regra vinculada ao serviço do Lambda.1.

Após a verificação inicial, a programação para cada controle pode ser periódica ou acionada por alterações.

- Verificações periódicas: essas verificações são executadas automaticamente em até 12 horas após a execução mais recente. O Security Hub determina a periodicidade, e você não pode alterá-la. Os controles periódicos refletem uma avaliação no momento em que a verificação é executada. Se você atualizar o status do fluxo de trabalho de uma descoberta de controle periódica e, na próxima verificação, o status de conformidade da descoberta permanecer o mesmo, o status do fluxo de trabalho permanecerá em seu estado modificado. Por exemplo, se você tiver uma falha na descoberta do KMS.4 - a AWS KMS key rotação deve ser ativada e, em seguida, corrigir a descoberta, o Security Hub alterará o status do fluxo de trabalho de para. `NEW` `RESOLVED` Se você desativar a alternância da chave KMS antes da próxima verificação periódica, o status do fluxo de trabalho da descoberta permanecerá `RESOLVED`.
- Verificações acionadas por alterações — Essas verificações são executadas quando o recurso associado muda de estado. AWS Config permite escolher entre gravação contínua de alterações no estado do recurso e gravação diária. Se você escolher a gravação diária, AWS Config fornecerá dados de configuração do recurso no final de cada período de 24 horas se houver alterações no estado do recurso. Se não houver alterações, nenhum dado será entregue. Isso pode atrasar a geração das descobertas do Security Hub até que um período de 24 horas seja concluído. Independentemente do período de gravação escolhido, o Security Hub verifica a cada 18 horas para garantir que nenhuma atualização de recursos tenha AWS Config sido perdida.

Em geral, o Security Hub usa regras acionadas por alterações sempre que possível. Para que um recurso use uma regra acionada por alterações, ele deve oferecer suporte a itens de AWS Config configuração.

Para um controle baseado em uma AWS Config regra gerenciada, a descrição do controle inclui um link para a descrição da regra no Guia do AWS Config desenvolvedor. Essa descrição inclui se a regra é periódica ou acionada por alterações.

As verificações que usam as funções do Lambda personalizadas para o Security Hub são periódicas.

Gerando e atualizando descobertas de controle

AWS Security Hub gera descobertas executando verificações em relação aos controles de segurança. Essas descobertas usam o AWS Security Finding Format (ASFF). Observe que, se o tamanho da descoberta exceder o máximo de 240 KB, o objeto `Resource.Details` será removido da descoberta. Para controles que são apoiados por AWS Config recursos, você pode ver os detalhes do recurso no AWS Config console.

O Security Hub normalmente cobra por cada verificação de segurança de um controle. No entanto, se vários controles usarem a mesma AWS Config regra, o Security Hub cobrará apenas uma vez por cada verificação contra a AWS Config regra. Se você ativar as descobertas de controle consolidadas, o Security Hub gerará uma única descoberta para uma verificação de segurança, mesmo quando o controle estiver incluído em vários padrões habilitados.

Por exemplo, a AWS Config regra `iam-password-policy` é usada por vários controles no padrão Center for Internet Security (CIS) AWS Foundations Benchmark e no padrão Foundational Security Best Practices. Cada vez que o Security Hub executa uma verificação em relação a essa AWS Config regra, ele gera uma descoberta separada para cada controle relacionado, mas cobra apenas uma vez pela verificação.

Ativar/desativar descobertas de controle consolidadas

Quando as descobertas de controle consolidadas são ativadas em sua conta, o Security Hub gera uma única nova descoberta ou atualização de descoberta para cada verificação de segurança de um controle, mesmo que um controle se aplique a vários padrões habilitados. Para ver uma lista dos controles e dos padrões aos quais eles se aplicam, consulte Referência de controles do Security Hub. Ativar/desativar descobertas de controle consolidadas Recomendamos ativá-lo para reduzir o ruído da descoberta.

Se você habilitou o Security Hub Conta da AWS antes de 23 de fevereiro de 2023, deverá ativar as descobertas de controle consolidadas seguindo as instruções mais adiante nesta seção. Se você ativar o Security Hub em ou após 23 de fevereiro de 2023, as descobertas de controle consolidadas serão ativadas automaticamente em sua conta. Entretanto, se você usar a integração do Security Hub com AWS Organizations ou convidar contas-membro por meio de um processo de convite manual, as descobertas de controle consolidadas serão ativadas nas contas dos membros somente se estiverem ativadas na conta do administrador. Se o atributo estiver desativado na conta do administrador, ele será desativado nas contas dos membros. Esse comportamento se aplica a contas-membro novas e existentes.

Se você desativar as descobertas de controle consolidadas em sua conta, o Security Hub gerará uma descoberta separada por verificação de segurança para cada padrão habilitado que inclui um controle. Por exemplo, se quatro padrões habilitados compartilharem um controle com a mesma AWS Config regra subjacente, você receberá quatro descobertas separadas após uma verificação de segurança do controle. Se você ativar as descobertas de controle consolidadas, receberá somente uma descoberta. Para obter mais informações sobre como a consolidação afeta suas descobertas, consulte Exemplo de descobertas de controle.

Quando você ativa as descobertas de controle consolidadas, o Security Hub cria novas descobertas independentes de padrões e arquiva as descobertas originais baseadas em padrões. Alguns campos e valores de busca de controle mudarão e poderão afetar os fluxos de trabalho existentes. Para mais informações sobre essas alterações, consulte Descobertas de controle consolidadas — Alterações no ASFF.

Ativar as descobertas de controle consolidadas também pode afetar as descobertas que as integrações de terceiros recebem do Security Hub. O Automated Security Response na AWS v2.0.0 oferece suporte a descobertas consolidadas de controle.

Ativar/desativar descobertas de controle consolidadas

Para ativar as descobertas de controle consolidadas, você deve estar conectado a uma conta de administrador ou a uma conta independente.

> **Note**
>
> Depois de ativar as descobertas de controle consolidadas, pode levar até 24 horas para que o Security Hub gere descobertas novas e consolidadas e arquive as descobertas originais baseadas em padrões. Durante esse período, será possível ver uma combinação de descobertas independentes de padrões e baseadas em padrões em sua conta.

Security Hub console

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, selecione Configurações.
3. Na guia General (Geral), escolha Edit (Editar).
4. Em Controles, ative as Descobertas de controle consolidadas.
5. Escolha Salvar.

Security Hub API

1. Executar UpdateSecurityHubConfiguration.
2. : não é igual a.

   Exemplo de solicitação

   ```
   {
      "ControlFindingGenerator": "SECURITY_CONTROL"
   }
   ```

AWS CLI

1. Execute o comando update-security-hub-configuration.
2. : não é igual a.

   ```
   aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
   ```

Ativar/desativar descobertas de controle consolidadas

Para ativar as descobertas de controle consolidadas, você deve estar conectado a uma conta de administrador ou a uma conta independente.

> **Note**
>
> Depois de ativar as descobertas de controle consolidadas, pode levar até 24 horas para que o Security Hub gere descobertas novas e consolidadas e arquive as descobertas originais baseadas em padrões. Durante esse período, será possível ver uma combinação de descobertas baseadas em padrões e consolidadas em sua conta.

Security Hub console

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, selecione Configurações.
3. Na guia General (Geral), escolha Edit (Editar).

4. Em Controles, selecione Editar e desative as Descobertas de controle consolidadas.
5. Escolha Salvar.

Security Hub API

1. Executar UpdateSecurityHubConfiguration.
2. : não é igual a.

   Exemplo de solicitação

```
{
   "ControlFindingGenerator": "STANDARD_CONTROL"
}
```

AWS CLI

1. Execute o comando update-security-hub-configuration.
2. : não é igual a.

```
aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

Detalhes **`Compliance`** das descobertas de controle

Para descobertas geradas por verificações de segurança de controles, o `Compliance`campo no Formato AWS de descoberta de segurança (ASFF) contém detalhes relacionados às descobertas de controle. O campo `Compliance` inclui as informações a seguir.

`AssociatedStandards`

Os padrões habilitados nos quais um controle está habilitado.

`RelatedRequirements`

A lista de requisitos relacionados para o controle em todos os padrões habilitados. Os requisitos são da estrutura de segurança de terceiros para o controle, como o Payment Card Industry Data Security Standard (PCI DSS).

`SecurityControlId`

O identificador para um controle entre os padrões de segurança que o Security Hub suporta.

`Status`

O resultado da verificação mais recente de que o Security Hub foi executado para um determinado controle. Os resultados das verificações anteriores são mantidos em um estado arquivado por 90 dias.

`StatusReasons`

Um objeto que contém uma lista de motivos para o valor de . Por cada motivo, `StatusReasons` inclui o código de motivo e uma descrição.

A tabela a seguir lista os códigos de motivo e descrições disponíveis. As etapas de correção dependem de qual controle gerou uma descoberta com o código do motivo. Escolha um controle no Referência de controles do Security Hub para ver as etapas de correção desse controle.

Código do motivo	Compliance.Status	Descrição
`CLOUDTRAIL_METRIC_FILTER_NOT_VALID`	`FAILED`	A CloudTrail trilha multirregional não tem um filtro métrico válido.
`CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT`	`FAILED`	Os filtros métricos não estão presentes na CloudTrail trilha multirregional.
`CLOUDTRAIL_MULTI_REGION_NOT_PRESENT`	`FAILED`	A conta não tem uma CloudTrail trilha multirregional com a configuração necessária.
`CLOUDTRAIL_REGION_INVAILD`	`WARNING`	As CloudTrail trilhas multirregionais não estão na região atual.
`CLOUDWATCH_ALARM_ACTIONS_NOT_VALID`	`FAILED`	Nenhuma ação de alarme válida está presente.

Código do motivo	Compliance.Status	Descrição
`CLOUDWATCH_ALARMS_NOT_PRESENT`	`FAILED`	CloudWatch os alarmes não existem na conta.
`CONFIG_ACCESS_DENIED`	`NOT_AVAILABLE` AWS Config status é `ConfigError`	AWS Config acesso negado. Verifique se AWS Config está ativado e se recebeu permissões suficientes.
`CONFIG_EVALUATIONS_EMPTY`	`PASSED`	AWS Config avaliou seus recursos com base na regra. A regra não se aplicava aos AWS recursos em seu escopo, os recursos especificados foram excluídos ou os resultados da avaliação foram excluídos.

Código do motivo	Compliance.Status	Descrição
`CONFIG_RETURNS_NOT_APPLICABLE`	`NOT_AVAILABLE`	O status de conformidade é `NOT_AVAILABLE` porque AWS Config retornou um status de Não aplicável. AWS Config não fornece o motivo do status. Aqui estão alguns motivos possíveis para o status Não aplicável: • O recurso foi removido do escopo da AWS Config regra. • A AWS Config regra foi excluída. • O recurso foi excluído. • A lógica da AWS Config regra pode produzir um status Não aplicável.

Código do motivo	Compliance.Status	Descrição
`CONFIG_RULE_EVALUATION_ERROR`	`NOT_AVAILABLE` AWS Config status é `ConfigError`	Esse código de motivo é usado para vários tipos diferentes de erros de avaliação. A descrição fornece as informações específicas do motivo. O tipo de erro pode ser um dos seguintes. • Uma incapacidade de realizar a avaliação devido à falta de permissões. A descrição fornece a permissão específica que está faltando. • Um valor ausente ou inválido para um parâmetro. A descrição fornece o parâmetro e os requisitos para o valor do parâmetro. • Erro ao ler a partir de um bucket do S3. A descrição identifica o bucket e fornece o erro específico. • Uma AWS assinatura ausente. • Um tempo limite geral para a avaliação. • Uma conta suspensa.
`CONFIG_RULE_NOT_FOUND`	`NOT_AVAILABLE` AWS Config status é `ConfigError`	A AWS Config regra está em processo de criação.

Código do motivo	Compliance.Status	Descrição
`INTERNAL_SERVICE_ERROR`	`NOT_AVAILABLE`	Ocorreu um erro desconhecido.
`LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE`	COM FALHA	O Security Hub não consegue realizar uma verificação em um runtime Lambda personalizado.
`S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION`	`WARNING`	A descoberta está em estado `WARNING` porque o bucket do S3 associado a essa regra está em uma região ou conta diferente. Essa regra não é compatível com verificações entre regiões ou entre contas. É recomendável que você desabilite esse controle nessa região ou conta. Execute somente na região ou na conta onde o recurso está localizado.
`SNS_SUBSCRIPTION_NOT_PRESENT`	`FAILED`	Os filtros métricos do CloudWatch Logs não têm uma assinatura válida do Amazon SNS.

Código do motivo	Compliance.Status	Descrição
SNS_TOPIC_CROSS_ACCOUNT	WARNING	A descoberta está em um estado de WARNING. O tópico SNS associado a esta regra pertence a uma conta diferente. A conta atual não pode obter as informações da assinatura. A conta proprietária do tópico do SNS deve conceder à conta atual a permissão sns:ListSubscriptionsByTopic para o tópico do SNS.
SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION	WARNING	A descoberta está em estado WARNING porque o tópico do SNS associado a essa regra está em uma região ou conta diferente. Essa regra não é compatível com verificações entre regiões ou entre contas. É recomendável que você desabilite esse controle nessa região ou conta. Execute somente na região ou na conta onde o recurso está localizado.
SNS_TOPIC_INVALID	FAILED	O tópico do SNS associado a essa regra é inválido.
THROTTLING_ERROR	NOT_AVAILABLE	A operação de API relevante excedeu a taxa permitida.

Detalhes **`ProductFields`** das descobertas de controle

Quando o Security Hub executa verificações de segurança e gera descobertas de controle, o atributo `ProductFields` no ASFF inclui os seguintes campos:

`ArchivalReasons:0/Description`

Descreve por que o Security Hub arquivou as descobertas existentes.

Por exemplo, o Security Hub arquiva descobertas existentes quando você desabilita um controle ou padrão e quando você ativa ou desativa descobertas de controle consolidadas.

`ArchivalReasons:0/ReasonCode`

Fornece o motivo pelo qual o Security Hub arquivou as descobertas existentes.

Por exemplo, o Security Hub arquiva descobertas existentes quando você desabilita um controle ou padrão e quando você ativa ou desativa descobertas de controle consolidadas.

`StandardsGuideArn` ou `StandardsArn`

O ARN do padrão associado ao controle.

Para o padrão CIS AWS Foundations Benchmark, o campo é. `StandardsGuideArn`

Para os padrões PCI DSS e AWS Foundational Security Best Practices, o campo é. `StandardsArn`

Esses campos serão removidos em favor de `Compliance.AssociatedStandards` se você ativar as descobertas de controle consolidadas.

`StandardsGuideSubscriptionArn` ou `StandardsSubscriptionArn`

O ARN da assinatura padrão da conta.

Para o padrão CIS AWS Foundations Benchmark, o campo é. `StandardsGuideSubscriptionArn`

Para os padrões PCI DSS e AWS Foundational Security Best Practices, o campo é. `StandardsSubscriptionArn`

Esses campos serão removidos em favor de se você ativar as descobertas de controle consolidadas.

`RuleId` ou `ControlId`

O identificador da .

Para o padrão CIS AWS Foundations Benchmark, o campo é. `RuleId`

Para outros padrões, o campo é `ControlId`.

Esses campos serão removidos em favor de `Compliance.SecurityControlId` se você ativar as descobertas de controle consolidadas.

`RecommendationUrl`

O URL para as informações de correção para o controle. Esses campos serão removidos em favor de `Remediation.Recommendation.Url` se você ativar as descobertas de controle consolidadas.

`RelatedAWSResources:0/name`

O que é associado ao tipo do recurso.

`RelatedAWSResource:0/type`

O que é associado ao tipo do recurso.

`StandardsControlArn`

O ARN do controle. Esse campo será removido se você ativar as descobertas de controle consolidadas.

`aws/securityhub/ProductName`

Para descobertas baseadas em controle, o nome do produto é Security Hub.

`aws/securityhub/CompanyName`

Para descobertas baseadas em controle, o nome da empresa é AWS.

`aws/securityhub/annotation`

Uma descrição do problema descoberto pelo controle.

`aws/securityhub/FindingId`

O identificador da . Esse campo não faz referência a um padrão se você ativar as descobertas de controle consolidadas.

Atribuir severidade às descobertas de controle

A severidade atribuída a um controle do Security Hub identifica a importância do controle. A severidade de um controle determina o rótulo de severidade atribuído às descobertas do controle.

Critérios de severidade

A severidade de um controle é determinada com base em uma avaliação dos seguintes critérios:

- É difícil para um agente de ameaças tirar proveito da fraqueza de configuração associada ao controle?

  A dificuldade é determinada pela quantidade de sofisticação ou complexidade necessária para usar a fraqueza para realizar um cenário de ameaça.
- Qual é a probabilidade de que a fraqueza leve ao comprometimento de seus recursos Contas da AWS ou de seus recursos?

  O comprometimento de seus Contas da AWS recursos significa que a confidencialidade, a integridade ou a disponibilidade de seus dados ou AWS infraestrutura estão danificadas de alguma forma.

  A probabilidade de comprometimento indica a probabilidade de o cenário de ameaça resultar em uma interrupção ou violação de seus AWS serviços ou recursos.

Como exemplo, considere os seguintes pontos fracos da configuração:

- As chaves de acesso do usuário não são trocadas a cada 90 dias.
- A chave de usuário raiz do IAM existe.

Ambas as fraquezas são igualmente difíceis de serem aproveitadas por um adversário. Em ambos os casos, o adversário pode usar o roubo de credenciais ou algum outro método para adquirir uma chave de usuário. Eles podem então usá-lo para acessar seus recursos de forma não autorizada.

Entretanto, a probabilidade de um comprometimento é muito maior se o agente da ameaça adquirir a chave de acesso do usuário raiz, pois isso lhe dá maior acesso. Como resultado, a fraqueza da chave do usuário raiz tem uma severidade maior.

A severidade não leva em conta a criticidade do recurso subjacente. A criticidade é definida como o nível de importância dos recursos associados à descoberta. Por exemplo, um recurso associado

a uma aplicação de missão crítica versus um associado a testes que não sejam de produção. Para capturar informações sobre a criticidade do recurso, use o `Criticality` campo AWS Security Finding Format (ASFF).

A tabela a seguir mapeia a dificuldade de exploração e a probabilidade de comprometimento dos rótulos de segurança.

	Comprometimento altamente provável	Comprometimento provável	Comprometimento provável	Comprometimento altamente provável
Muito fácil de explorar	Crítico	Crítico	Alta	Médio
Um pouco fácil de explorar	Crítico	Alta	Médio	Médio
Um pouco difícil de explorar	Alta	Médio	Médio	Baixo
Muito difícil de explorar	Médio	Médio	Baixo	Baixo

Definições de severidade

Os rótulos de severidade são definidos da seguinte forma.

CRÍTICA: o problema deve ser corrigido imediatamente para evitar que seja escalonado.

> Por exemplo, um bucket do S3 aberto é considerado uma descoberta de gravidade crítica. Como muitos usuários examinam buckets do S3 abertos, é provável que os dados em um bucket do S3 exposto sejam descobertos e acessados por outros.
>
> Em geral, os recursos acessíveis ao público são considerados problemas críticos de segurança. Você deve tratar as descobertas críticas com a máxima urgência. Você também deve considerar a importância do recurso.

ALTA: o problema deve ser tratado como prioridade.

Por exemplo, se um grupo de segurança VPC padrão estiver aberto ao tráfego de entrada e saída, ele será considerado de alta severidade. É um pouco fácil para um agente de ameaças comprometer uma VPC usando esse método. Também é provável que o agente da ameaça consiga interromper ou exfiltrar recursos quando eles estiverem na VPC.

O Security Hub recomenda que você trate uma descoberta de alta severidade como uma prioridade de curto prazo. Você deve tomar medidas imediatas de correção. Você também deve considerar a importância do recurso.

Médio — A questão deve ser tratada como uma prioridade de médio prazo.

Por exemplo, a falta de criptografia para dados em trânsito é considerada uma descoberta de severidade média. É necessário um man-in-the-middle ataque sofisticado para tirar proveito dessa fraqueza. Em outras palavras, é um pouco difícil. É provável que alguns dados sejam comprometidos se o cenário de ameaça for bem-sucedido.

Recomendamos que você investigue o recurso implicado o mais cedo possível. Você também deve considerar a importância do recurso.

o problema não requer ação por conta própria.

Por exemplo, a falha na coleta de informações forenses é considerada de baixa severidade. Esse controle pode ajudar a evitar futuros compromissos, mas a ausência de perícia não leva diretamente a um comprometimento.

Você não precisa tomar medidas imediatas em relação às descobertas de baixa severidade, mas elas podem fornecer contexto quando você as correlaciona com outros problemas.

Informativo — Nenhuma falha de configuração foi encontrada.

Em outras palavras, o status é .

Não há ação recomendada. As descobertas informativas ajudam os clientes a demonstrar que estão em um estado de conformidade.

Regras para atualizar as descobertas de controle

Uma verificação subsequente em relação a uma determinada regra pode gerar um novo resultado. Por exemplo, o status de “Evitar o uso do usuário raiz” pode mudar de `FAILED` para `PASSED`. Nesse caso, é gerada uma nova descoberta contendo o resultado mais recente.

Se uma verificação subsequente com base em uma determinada regra gerar um resultado idêntico ao resultado atual, a descoberta existente será atualizada. Nenhuma nova descoberta será gerada.

O Security Hub arquiva automaticamente as descobertas dos controles se o recurso associado for excluído, se o recurso não existir ou se o controle estiver desabilitado. Um recurso pode não existir mais porque o serviço associado não está sendo usado no momento. As descobertas são arquivadas automaticamente com base em um dos seguintes critérios:

- A descoberta não é atualizada em três a cinco dias (observe que esse é a melhor tentativa e não é garantida).
- A AWS Config avaliação associada retornou`NOT_APPLICABLE`.

Status de conformidade e status de controle

O `Compliance.Status` campo do Formato de descoberta de AWS segurança descreve o resultado de uma descoberta de controle. O Security Hub usa o status de conformidade das descobertas de controle para determinar um status geral de controle. O status do controle é exibido na página de detalhes de um controle no console do Security Hub.

Para uma conta de administrador, o status de controle reflete o status de controle na conta do administrador e nas contas dos membros. Especificamente, o status geral de um controle aparece como Falha se o controle tiver uma ou mais descobertas malsucedidas na conta do administrador ou em qualquer uma das contas dos membros. Se você tiver definido uma Região de agregação, o status de controle na Região de agregação refletirá o status de controle na Região de agregação e nas Regiões vinculadas. Especificamente, o status geral de um controle aparece como Falha se o controle tiver uma ou mais descobertas com falha na região de agregação ou em qualquer uma das regiões vinculadas.

Normalmente, o Security Hub gera o status de controle inicial dentro de 30 minutos após sua primeira visita à página Resumo ou à página Padrões de segurança do console do Security Hub. Você deve ter a gravação AWS Config de recursos configurada para que o status do controle apareça. Depois que os status de controle são gerados pela primeira vez, o Security Hub atualiza os status de controle a cada 24 horas com base nas descobertas das 24 horas anteriores. Um carimbo de data/hora na página de detalhes do controle indica quando o status do controle foi atualizado pela última vez.

> **Note**
>
> Pode levar até 24 horas após a ativação de um controle para que os primeiros status de controle sejam gerados nas regiões da China e AWS GovCloud (US) Region.

Valores do status de conformidade de uma descoberta

O status de conformidade de cada descoberta é atribuído a um dos seguintes valores:

- `PASSED`— Indica que o controle passou na verificação de segurança dessa descoberta. Define automaticamente o Security Hub `Workflow.Status` como`RESOLVED`.

  Se `Compliance.Status` para uma descoberta mudar de`PASSED`,, ou `FAILED` `WARNING``NOT_AVAILABLE`, e `Workflow.Status` for um ou `NOTIFIED``RESOLVED`, o Security Hub será configurado automaticamente `Workflow.Status` como`NEW`.

  Se você não tiver recursos correspondentes a um controle, o Security Hub produzirá uma `PASSED` descoberta no nível da conta. Se você tiver um recurso correspondente a um controle, mas depois excluir o recurso, o Security Hub cria uma `NOT_AVAILABLE` descoberta e a arquiva imediatamente. Após 18 horas, você recebe uma `PASSED` descoberta, pois não tem mais recursos correspondentes ao controle.
- `FAILED`— Indica que o controle não passou na verificação de segurança dessa descoberta.
- `WARNING`— Indica que a verificação foi concluída, mas o Security Hub não consegue determinar se o recurso está em um `FAILED` estado `PASSED` ou.
- `NOT_AVAILABLE`— Indica que a verificação não pode ser concluída porque um servidor falhou, o recurso foi excluído ou o resultado da AWS Config avaliação foi`NOT_APPLICABLE`.

  Se o resultado da AWS Config avaliação for`NOT_APPLICABLE`, o Security Hub arquiva automaticamente a descoberta.

Valores para status de controle

O Security Hub deriva um status geral de controle do status de conformidade das descobertas de controle. Ao determinar o status do controle, o Security Hub ignora as descobertas que têm um `RecordState` de `ARCHIVED` e as descobertas que têm um `Workflow.Status` de`SUPPRESSED`.

O status do controle é atribuído a um dos seguintes valores:

- Aprovado — Indica que todas as descobertas têm um status de conformidade de`PASSED`.
- Falha — Indica que pelo menos uma descoberta tem um status de conformidade de`FAILED`.
- Desconhecido — Indica que pelo menos uma descoberta tem um status de conformidade de `WARNING` ou`NOT_AVAILABLE`. Nenhuma descoberta tem um status de conformidade de`FAILED`.
- Sem dados — Indica que não há descobertas para o controle. Por exemplo, um controle recém-ativado tem esse status até que o Security Hub comece a gerar descobertas para ele. Um controle também tem esse status se todas as descobertas estiverem `SUPPRESSED` ou não estiverem disponíveis na região atual.
- Desativado — Indica que o controle está desativado na conta atual e na região. Nenhuma verificação de segurança está sendo executada atualmente para esse controle na conta corrente e na região. No entanto, as descobertas de um controle desativado podem ter um valor para o status de conformidade por até 24 horas após a desativação.

Determinando as pontuações de segurança

A página Resumo e a página Controles do console do Security Hub exibem uma pontuação de segurança resumida em todos os padrões habilitados. Na página Padrões de segurança, o Security Hub também exibe uma pontuação de segurança de 0 a 100% para cada padrão habilitado.

Quando você habilita o Security Hub pela primeira vez, o Security Hub calcula a pontuação de segurança resumida e as pontuações de segurança padrão dentro de 30 minutos após sua primeira visita à página Resumo ou à página Padrões de Segurança no console do Security Hub. As pontuações são geradas somente para padrões que são ativados quando você visita essas páginas. Para ver uma lista dos padrões atualmente habilitados, invoque a operação da API `GetEnabledStandards`. Além disso, o registro AWS Config de recursos deve ser configurado para que as pontuações apareçam. A pontuação de segurança resumida é a média das pontuações de segurança padrão.

Após a primeira geração de pontuação, o Security Hub atualiza as pontuações de segurança a cada 24 horas. O Security Hub exibe um timestamp para indicar quando uma pontuação de segurança foi atualizada pela última vez.

> **Note**
>
> Pode levar até 24 horas para que as pontuações de segurança pela primeira vez sejam geradas nas regiões da China e AWS GovCloud (US) Region.

Se você ativar as descobertas de controle consolidadas, poderá levar até 24 horas para que suas pontuações de segurança sejam atualizadas. Além disso, habilitar uma nova região de agregação ou atualizar regiões vinculadas redefine as pontuações de segurança existentes. Pode levar até 24 horas para que o Security Hub gere novas pontuações de segurança que incluam dados das regiões atualizadas.

Como as pontuações de segurança são calculadas

A pontuação de segurança representa a proporção de controles no estado Passed (Aprovado) para controles habilitados. A pontuação é exibida como uma porcentagem arredondada para cima ou para baixo para o número inteiro mais próximo.

O Security Hub calcula uma pontuação de segurança resumida em todos os seus padrões habilitados. O Security Hub também calcula uma pontuação de segurança em todos os controles habilitados e para padrões específicos. Para fins de cálculo de pontuação, os controles habilitados incluem controles com status de Aprovado, Falha e Desconhecido. Os controles com o status Sem dados são excluídos do cálculo da pontuação.

O Security Hub ignora descobertas arquivadas e suprimidas ao calcular o status do controle. Isso pode afetar as pontuações de segurança. Por exemplo, se você suprimir todas as descobertas malsucedidas de um controle, seu status se tornará Aprovado, o que, por sua vez, pode melhorar suas pontuações de segurança. Para obter mais informações sobre tabelas de controle, consulte Status de conformidade e status de controle.

Exemplo de pontuação:

Padrão	Controles aprovados	Falha nos controles	Controles desconhecidos	Escopos-padrão
AWS Melhores práticas básicas de segurança v1.0.0	168	22	0	88%
Referência do CIS AWS Foundations v1.4.0	8	29	0	22%

Padrão	Controles aprovados	Falha nos controles	Controles desconhecidos	Escopos-padrão
Referência do CIS AWS Foundations v1.2.0	6	35	0	15%
Publicação especial 800-53 do NIST Revisão 5	159	56	0	74%
PCI DSS v3.2.1	28	17	0	62%

Ao calcular a pontuação resumida de segurança, o Security Hub conta cada controle apenas uma vez em todos os padrões. Por exemplo, se você ativou um controle que se aplica a três padrões ativados, ele conta apenas como um controle ativado para fins de pontuação.

Neste exemplo, embora o número total de controles habilitados em todos os padrões habilitados seja 528, o Security Hub conta cada controle exclusivo apenas uma vez para fins de pontuação. O número de controles ativados exclusivos provavelmente é menor que 528. Se assumirmos que o número de controles exclusivos ativados é 515 e o número de controles exclusivos aprovados é 357, a pontuação resumida é 69%. Essa pontuação é calculada dividindo o número de controles exclusivos aprovados pelo número de controles exclusivos habilitados.

É possível ter uma pontuação resumida diferente da pontuação de segurança padrão, mesmo que tenha ativado apenas um padrão em sua conta na região atual. Isso pode ocorrer se você estiver conectado a uma conta de administrador e as contas-membro tiverem padrões adicionais ou padrões diferentes ativados. Isso também pode ocorrer se você estiver visualizando a pontuação da região de agregação e padrões adicionais ou padrões diferentes estiverem ativados nas regiões vinculadas.

Pontuações de segurança para contas de administrador

Se você estiver conectado a uma conta de administrador, a pontuação de segurança resumida e a pontuação padrão contam com os status de controle na conta do administrador e em todas as contas dos membros.

Se o status de um controle for Falha em até mesmo uma conta-membro, seu status será Falha na conta do administrador e afetará as pontuações da conta do administrador.

Se você estiver conectado a uma conta de administrador e estiver visualizando pontuações em uma região de agregação, as pontuações de segurança representam os status de controle em todas as contas-membro e em todas as regiões vinculadas.

Pontuações de segurança se você tiver definido uma região de agregação

Se você definiu uma agregação Região da AWS, a pontuação de segurança resumida e a pontuação padrão são responsáveis pelos status de controle em todos Regiões vinculadas.

Se o status de um controle for Falha em até mesmo uma região vinculada, seu status será Falha na região de agregação e afetará as pontuações da região de agregação.

Se você estiver conectado a uma conta de administrador e estiver visualizando pontuações em uma região de agregação, as pontuações de segurança representam os status de controle em todas as contas-membro e em todas as regiões vinculadas.

Referência de padrões do Security Hub

AWS Security Hub atualmente suporta os padrões de segurança detalhados nesta seção.

Escolha um padrão para ver mais detalhes sobre ele e os controles que se aplicam a ele.

Os padrões e controles do Security Hub não garantem a conformidade com nenhuma estrutura regulatória ou auditoria. Em vez disso, os controles fornecem uma forma de monitorar o estado atual de suas Contas da AWS e recursos.

Padrões compatíveis com o

- AWS Padrão Foundational Security Best Practices (FSBP)
- Referências do CIS AWS Foundations
- Instituto Nacional de Padrões e Tecnologia (National Institute of Standards and Technology, NIST) SP 800-53 (Revisão 4)
- Padrão de segurança de dados do setor de cartão de pagamento (PCI DSS – Payment Card Industry Data Security Standard)
- AWS Padrão de marcação de recursos
- Padrões gerenciados por serviços

AWS Padrão Foundational Security Best Practices (FSBP)

O padrão AWS Foundational Security Best Practices é um conjunto de controles que detectam quando você Contas da AWS e seus recursos se desviam das melhores práticas de segurança.

O padrão permite que você avalie continuamente todas as suas cargas de trabalho Contas da AWS e suas cargas de trabalho para identificar rapidamente as áreas de desvio das melhores práticas. Ele fornece orientações acionáveis e prescritivas sobre como aprimorar e manter a postura de segurança da sua organização.

Os controles incluem as melhores práticas de segurança para recursos de vários Serviços da AWS. Cada controle recebe uma categoria que reflete a função de segurança à qual ele se aplica. Para ter mais informações, consulte the section called “Categorias de controle”.

Controles que se aplicam ao padrão FSBP

[Conta.1] As informações de contato de segurança devem ser fornecidas para um Conta da AWS

Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado

Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits

[ApiGateway.1] O REST do API Gateway WebSocket e o registro de execução da API devem estar habilitados

Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end

Os estágios da API REST de Gateway devem ter o rastreamento AWS X-Ray habilitado.

O API Gateway deve ser associado a uma WAF Web ACL

Os dados do cache da API REST de Gateway devem ser criptografados em repouso

As rotas do API de Gateway devem especificar um tipo de autorização

O registro de acesso deve ser configurado para os estágios V2 do API de Gateway

[AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado

[AppSync.5] As APIs AWS AppSync do GraphQL não devem ser autenticadas com chaves de API

[AutoScaling.1] Grupos de Auto Scaling associados a um balanceador de carga devem usar verificações de integridade do ELB

[AutoScaling.2] O grupo Amazon EC2 Auto Scaling deve abranger várias zonas de disponibilidade

[AutoScaling.3] As configurações de lançamento de grupos do Auto Scaling devem configurar as instâncias do EC2 para exigir o Instance Metadata Service Version 2 (IMDSv2)

As instâncias do Amazon EC2 lançadas usando as configurações de execução em grupo do Auto Scaling não devem ter endereços IP públicos

[AutoScaling.6] Os grupos de Auto Scaling devem usar vários tipos de instância em várias zonas de disponibilidade

[AutoScaling.9] Os grupos do Amazon EC2 Auto Scaling devem usar os modelos de lançamento do Amazon EC2

[Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso

[CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado

[CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito

[CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado

[CloudFront.5] CloudFront as distribuições devem ter o registro ativado

[CloudFront.6] as CloudFront distribuições devem ter o WAF ativado

[CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados

[CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS

[CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas

[CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas

[CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3

[CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem

[CloudTrail.1] CloudTrail deve ser habilitado e configurado com pelo menos uma trilha multirregional que inclua eventos de gerenciamento de leitura e gravação

[CloudTrail.2] CloudTrail deve ter a criptografia em repouso ativada

[CloudTrail.4] a validação do arquivo de CloudTrail log deve estar ativada

[CloudTrail.5] CloudTrail trilhas devem ser integradas com o Amazon CloudWatch Logs

[CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais

[CodeBuild.2] as variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado

[CodeBuild.3] Os registros do CodeBuild S3 devem ser criptografados

[CodeBuild.4] ambientes de CodeBuild projeto devem ter uma duração de registro AWS Config

[Config.1] AWS Config deve estar habilitado

[DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso

As instâncias de replicação do PCI.DMS.1 Database Migration Service não devem ser públicas

As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada

As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado

As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado

Os endpoints do DMS devem usar SSL

[DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada

[DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado

[DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado

Os clusters do Amazon DocumentDB devem ser criptografados em repouso

Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado

Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos

[DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch

Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada

As tabelas do DynamoDB devem escalar automaticamente a capacidade de acordo com a demanda

[DynamoDB.2] As tabelas do DynamoDB devem ter a recuperação ativada point-in-time

Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso

[DynamoDB.6] As tabelas do DynamoDB devem ter a proteção contra exclusão habilitada

[DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito

[PCI.EC2.1] Os instantâneos do Amazon EBS não devem ser restauráveis publicamente

[EC2.2] O grupo de segurança padrão da VPC não deve permitir o tráfego de entrada e saída

[EC2.3] Os volumes anexados do Amazon EBS devem ser criptografados em repouso.

As instâncias EC2 interrompidas devem ser removidas após um período de tempo especificado

[EC2.6] O registro de fluxo de VPC deve ser ativado em todas as VPCs

[EC2.7] A criptografia padrão do EBS deve estar ativada

As instâncias do EC2 devem usar o Instance Metadata Service Version 2 (IMDSv2)

As instâncias do Amazon EC2 não devem ter um endereço IPv4 público

O Amazon EC2 deve ser configurado para usar endpoints da VPC criados para o serviço Amazon EC2

As sub-redes do Amazon EC2 não devem atribuir automaticamente endereços IP públicos

As listas de controle de acesso à rede não utilizadas devem ser removidas

As instâncias do Amazon EC2 não devem usar vários ENIs

Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas

Grupos de segurança não devem permitir acesso irrestrito a portas com alto risco

[EC2.20] Ambos os túneis VPN para uma conexão VPN Site-to-Site devem estar ativos AWS

As ACLs de rede não devem permitir a entrada de 0.0.0.0/0 para a porta 22 ou porta 3389

Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC

Os tipos de instância paravirtual do Amazon EC2 não devem ser usados

Os modelos de lançamento do Amazon EC2 não devem atribuir IPs públicos às interfaces de rede

[EC2.51] Os endpoints da Client VPN do EC2 devem ter o registro em log de conexão do cliente habilitado

Os repositórios privados do ECR devem ter a digitalização de imagens configurada

[ECR.2] Os repositórios privados do ECR devem ter a imutabilidade da tag configurada

Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada

As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário.

Os serviços do ECS não devem ter endereços IP públicos atribuídos a eles automaticamente

As definições de tarefas do ECS não devem compartilhar o namespace do processo do host

Os contêineres ECS devem ser executados sem privilégios

Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz

Os segredos não devem ser passados como variáveis de ambiente do contêiner

As definições de tarefas do ECS devem ter uma configuração de registro em log

Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate

Os clusters do ECS devem usar Container Insights

[EFS.1] O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS

[EFS.2] Os volumes do Amazon EFS devem estar em planos de backup

Os pontos de acesso do EFS devem impor um diretório raiz

Os pontos de acesso do EFS devem impor uma identidade de usuário

[EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública

Os endpoints do cluster EKS não devem ser acessíveis ao público

Os clusters EKS devem ser executados em uma versão compatível do Kubernetes

[EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes

[EKS.8] Os clusters do EKS devem ter o registro em log de auditoria habilitado

[ElastiCache.1] Os clusters ElastiCache Redis devem ter o backup automático ativado

[ElastiCache.2] ElastiCache para clusters de cache Redis deve ter a atualização automática de versão secundária habilitada

[ElastiCache.3] ElastiCache para grupos de replicação do Redis, o failover automático deve estar ativado

[ElastiCache.4] ElastiCache para Redis, os grupos de replicação devem ser criptografados em repouso

[ElastiCache.5] ElastiCache para Redis, os grupos de replicação devem ser criptografados em trânsito

[ElastiCache.6] ElastiCache para grupos de replicação do Redis antes da versão 6.0 deve usar o Redis AUTH

[ElastiCache.7] os ElastiCache clusters não devem usar o grupo de sub-rede padrão

[ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de integridade aprimorados habilitados

[ElasticBeanstalk.2] As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas

[ElasticBeanstalk.3] O Elastic Beanstalk deve transmitir registros para CloudWatch

[ELBv2.1] O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS

[ELB.2] Os balanceadores de carga clássicos com ouvintes SSL/HTTPS devem usar um certificado fornecido pelo AWS Certificate Manager

Os receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS

O Application Load Balancer deve ser configurado para eliminar cabeçalhos http

O registro em log do Classic Load Balancer e Application Load Balancer deve estar ativado

[ELB.6] Os balanceadores de carga de aplicativos, gateways e redes devem ter a proteção contra exclusão ativada

Os Classic Load Balancers devem ter a drenagem da conexão ativada

[ELB.8] Os balanceadores de carga clássicos com ouvintes SSL devem usar uma política de segurança predefinida que tenha uma duração forte AWS Config

Os Classic Load Balancers devem ter o balanceador de carga entre zonas habilitado

Verifica se o Classic Load Balancer abrange várias zonas de disponibilidade (AZs).

O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso

Balanceadores de carga de aplicações, redes e gateways não abrangem várias zonas de disponibilidade

O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso

[EMR.1] Os nós primários do cluster do Amazon EMR não devem ter endereços IP públicos

[EMR.2] A configuração de bloqueio de acesso público do Amazon EMR deve estar habilitada

[ES.1] Os domínios do devem ter a criptografia em repouso habilitada.

[ES.2] Os domínios do Elasticsearch não devem ser publicamente acessíveis

Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós

[ES.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado

Os domínios do Elasticsearch devem ter o registro em log de auditoria ativado

Os domínios do Elasticsearch devem ter pelo menos três nós de dados

Os domínios do Elasticsearch devem ser configurados com pelo menos três nós principais dedicados

[ES.8] As conexões com os domínios do Elasticsearch devem ser criptografadas usando a política de segurança TLS mais recente

[EventBridge.3] os ônibus de eventos EventBridge personalizados devem ter uma política baseada em recursos anexada

[FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.

[FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups

[GuardDuty.1] GuardDuty deve ser ativado

[IAM.1] As políticas do não devem permitir privilégios administrativos completos "*"

[IAM.2] Os usuários do não devem ter políticas do IAM anexadas

[IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos

[IAM.4] A chave de acesso do usuário raiz do não deve existir

[IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console

[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz

[IAM.7] As políticas de senha para usuários do IAM devem ter configurações fortes

As credenciais de usuário do IAM não utilizadas devem ser removidas

As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.

Os fluxos do Kinesis devem ser criptografados em repouso

As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS

As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS

[KMS.3] não AWS KMS keys deve ser excluído acidentalmente

[PCI.lambda.1] As funções do devem proibir o acesso público

[Lambda.2] As funções do devem usar os tempos de execução mais recentes

[Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade

[Macie.1] O Amazon Macie deve estar ativado

[Macie.2] A descoberta automatizada de dados confidenciais do Macie deve ser ativada

[MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch

[MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada

Os clusters MSK devem ser criptografados em trânsito entre os nós do agente

Os clusters de banco de dados Neptune devem ser criptografados em repouso

[Neptune.2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch

Os instantâneos do cluster de banco de dados Neptune não devem ser públicos

[Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada

Os clusters de banco de dados Neptune devem ter backups automatizados habilitados

Os clusters de banco de dados Neptune devem ser criptografados em repouso

[Neptune.7] Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada

Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos

[NetworkFirewall.2] O registro do Firewall de Rede deve estar ativado

[NetworkFirewall.3] As políticas de Firewall de Rede devem ter pelo menos um grupo de regras associado

[NetworkFirewall.4] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar pacotes completos

[NetworkFirewall.5] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar para pacotes fragmentados

[NetworkFirewall.6] O grupo de regras do Stateless Network Firewall não deve estar vazio

[NetworkFirewall.9] Os firewalls do Firewall de Rede devem ter a proteção contra exclusão ativada

Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada

Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público

Os OpenSearch domínios [Opensearch.3] devem criptografar os dados enviados entre os nós

O registro de erros de OpenSearch domínio [Opensearch.4] nos CloudWatch registros deve estar ativado

Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado

Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados

Os OpenSearch domínios [Opensearch.7] devem ter um controle de acesso refinado ativado

[Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente

Os OpenSearch domínios [Opensearch.10] devem ter a atualização de software mais recente instalada

[PCA.1] a autoridade de certificação AWS Private CA raiz deve ser desativada

As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS

[RDS.1] Os instantâneos do RDS devem ser privados

[RDS.2] As instâncias de banco de dados do RDS devem proibir o acesso público, conforme determinado pela duração PubliclyAccessible AWS Config

[RDS.3] As instâncias de banco de dados do RDS devem ter a criptografia em repouso habilitada.

Os instantâneos do cluster do RDS e os instantâneos do banco de dados devem ser criptografados em repouso

As instâncias de banco de dados do RDS devem ser configuradas com várias zonas de disponibilidade

O monitoramento aprimorado deve ser configurado para instâncias de banco de dados do RDS

[RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada

[RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada

[RDS.9] As instâncias de banco de dados do RDS devem publicar registros no Logs CloudWatch

A autenticação do IAM deve ser configurada para instâncias do RDS

As instâncias do RDS devem ter backups automáticos habilitados

A autenticação do IAM deve ser configurada para instâncias do RDS

[RDS.13] As atualizações automáticas de versões secundárias do RDS devem ser ativadas

[RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado

[RDS.15] Os clusters de banco de dados do RDS devem ser configurados para várias zonas de disponibilidade

Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos

As instâncias de banco de dados do RDS devem ser configuradas para copiar tags para instantâneos

As instâncias do RDS devem ser implantadas em uma VPC

As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de cluster

As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de cluster

Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de parâmetros do banco de dados

Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de parâmetros do banco de dados

As instâncias do RDS não devem usar uma porta padrão do mecanismo de banco de dados

Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado

Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado

Os clusters de banco de dados Neptune devem ser criptografados em repouso

[RDS.34] Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch

Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada

[PCI.Redshift.1] Os clusters do devem proibir o acesso público

As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito

Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados

Os clusters do Amazon Redshift devem ter o registro de auditoria ativado

O Amazon Redshift deve ter as atualizações automáticas para as versões principais habilitadas

Os clusters do Redshift devem usar roteamento de VPC aprimorado

Os clusters do Amazon Redshift não devem usar o nome de usuário Admin padrão

[Redshift.9] Os clusters do Redshift não devem usar o nome do banco de dados padrão

[Redshift.10] Os clusters do Redshift devem ser criptografados em repouso

[Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas

[S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas

[S3.2] Os buckets de uso geral do S3 devem bloquear o acesso público de leitura

[S3.3] Os buckets de uso geral do S3 devem bloquear o acesso público de gravação

[S3.5] Os buckets de uso geral do S3 devem exigir solicitações de uso de SSL

[S3.6] As políticas de bucket de uso geral do S3 devem restringir o acesso a outros Contas da AWS

[S3.8] Os buckets de uso geral do S3 devem bloquear o acesso público

[S3.9] Os buckets de uso geral do S3 devem ter o registro de acesso ao servidor ativado

[S3.12] As ACLs não devem ser usadas para gerenciar o acesso do usuário aos buckets de uso geral do S3

[S3.13] Os buckets de uso geral do S3 devem ter configurações de ciclo de vida

[S3.19] Os pontos de acesso do S3 devem ter configurações de bloqueio do acesso público habilitadas

[SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet

[SageMaker.2] as instâncias do SageMaker notebook devem ser iniciadas em uma VPC personalizada

[SageMaker.3] Os usuários não devem ter acesso root às instâncias do SageMaker notebook

[SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1

[SecretsManager.1] Os segredos do Secrets Manager devem ter a rotação automática ativada

[SecretsManager.2] Os segredos do Secrets Manager configurados com rotação automática devem girar com sucesso

[SecretsManager.3] Remover segredos não utilizados do Secrets Manager

[SecretsManager.4] Os segredos do Secrets Manager devem ser alternados dentro de um determinado número de dias

[ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS

As filas do Amazon SQS devem ser criptografadas em repouso

[SSM.1] As instâncias do Amazon EC2 devem ser gerenciadas por AWS Systems Manager

[PCI.SSM.1] As instâncias do Amazon EC2 gerenciadas pelo devem ter um status de conformidade de patch de COMPLIANT (Em conformidade) após a instalação do patch

PCI.SSM.2 As instâncias de Amazon EC2 gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL

Os documentos SSM não devem ser públicos

[StepFunctions.1] As máquinas de estado do Step Functions devem ter o registro ativado

[Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints

[WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado

[WAF.2] As regras regionais AWS WAF clássicas devem ter pelo menos uma condição

[WAF.3] Os grupos de regras regionais AWS WAF clássicos devem ter pelo menos uma regra

[WAF.4] As ACLs regionais AWS WAF clássicas da web devem ter pelo menos uma regra ou grupo de regras

[WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição

[WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra

[WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

[WAF.10] as ACLs AWS WAF da web devem ter pelo menos uma regra ou grupo de regras

As AWS WAF regras [WAF.12] devem ter métricas habilitadas CloudWatch

Referências do CIS AWS Foundations

O Center for Internet Security (CIS) AWS Foundations Benchmark serve como um conjunto de melhores práticas de configuração de segurança para. AWS Essas melhores práticas aceitas pelo setor fornecem procedimentos claros de step-by-step implementação e avaliação. Variando de sistemas operacionais a serviços em nuvem e dispositivos de rede, as configurações aplicadas a partir de um benchmark protegem os sistemas específicos que sua organização usa.

AWS Security Hub suporta o CIS AWS Foundations Benchmark v3.0.0, 1.4.0 e v1.2.0.

Esta página lista os controles de segurança que cada versão suporta e fornece uma comparação das versões.

Referência do CIS AWS Foundations v3.0.0

O Security Hub é compatível com a versão 3.0.0 do CIS AWS Foundations Benchmark.

O satisfez os requisitos de segurança do CIS Software Certification e recebeu a CIS Security Software Certification para as seguintes referências da CIS:

- Benchmark CIS para CIS AWS Foundations Benchmark, v3.0.0, Nível 1
- Benchmark CIS para CIS AWS Foundations Benchmark, v3.0.0, Nível 2

Controles que se aplicam ao CIS AWS Foundations Benchmark v3.0.0

[Conta.1] As informações de contato de segurança devem ser fornecidas para um Conta da AWS

[CloudTrail.1] CloudTrail deve ser habilitado e configurado com pelo menos uma trilha multirregional que inclua eventos de gerenciamento de leitura e gravação

[CloudTrail.2] CloudTrail deve ter a criptografia em repouso ativada

[CloudTrail.4] a validação do arquivo de CloudTrail log deve estar ativada

[CloudTrail.7] Certifique-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrail S3

[Config.1] AWS Config deve estar habilitado

[EC2.2] O grupo de segurança padrão da VPC não deve permitir o tráfego de entrada e saída

[EC2.6] O registro de fluxo de VPC deve ser ativado em todas as VPCs

[EC2.7] A criptografia padrão do EBS deve estar ativada

As instâncias do EC2 devem usar o Instance Metadata Service Version 2 (IMDSv2)

As ACLs de rede não devem permitir a entrada de 0.0.0.0/0 para a porta 22 ou porta 3389

[EC2.53] Os grupos de segurança do EC2 não devem permitir a entrada de 0.0.0.0/0 nas portas de administração remota do servidor

[EC2.54] Os grupos de segurança do EC2 não devem permitir a entrada de: :/0 nas portas de administração do servidor remoto

[EFS.1] O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS

[IAM.2] Os usuários do não devem ter políticas do IAM anexadas

[IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos

[IAM.4] A chave de acesso do usuário raiz do não deve existir

[IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console

[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz

[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz

1.9 Certifique-se de que a política de senha do IAM exija um comprimento mínimo de 14 ou mais

1.10 Certifique-se de que a política de senha do IAM impeça a reutilização de senhas

[IAM.18] Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support

As credenciais de usuário do IAM não utilizadas devem ser removidas

[IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos

[IAM.27] As identidades do IAM não devem ter a política anexada AWSCloudShellFullAccess

[IAM.28] O analisador de acesso externo do IAM Access Analyzer deve estar ativado

A rotação de AWS KMS teclas [KMS.4] deve estar ativada

[RDS.2] As instâncias de banco de dados do RDS devem proibir o acesso público, conforme determinado pela duração PubliclyAccessible AWS Config

[RDS.3] As instâncias de banco de dados do RDS devem ter a criptografia em repouso habilitada.

[RDS.13] As atualizações automáticas de versões secundárias do RDS devem ser ativadas

[S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas

[S3.5] Os buckets de uso geral do S3 devem exigir solicitações de uso de SSL

[S3.8] Os buckets de uso geral do S3 devem bloquear o acesso público

[S3.20] Os buckets de uso geral do S3 devem ter a exclusão de MFA habilitada

[S3.22] Os buckets de uso geral do S3 devem registrar eventos de gravação em nível de objeto

[S3.23] Os buckets de uso geral do S3 devem registrar eventos de leitura em nível de objeto

Referência do CIS AWS Foundations v1.4.0

O Security Hub é compatível com a versão 1.4.0 do CIS Foundations Benchmark AWS .

Controles que se aplicam ao CIS AWS Foundations Benchmark v1.4.0

[CloudTrail.1] CloudTrail deve ser habilitado e configurado com pelo menos uma trilha multirregional que inclua eventos de gerenciamento de leitura e gravação

[CloudTrail.2] CloudTrail deve ter a criptografia em repouso ativada

[CloudTrail.4] a validação do arquivo de CloudTrail log deve estar ativada

[CloudTrail.5] CloudTrail trilhas devem ser integradas com o Amazon CloudWatch Logs

[CloudTrail.6] Certifique-se de que o bucket do S3 usado para armazenar CloudTrail registros não esteja acessível ao público

[CloudTrail.7] Certifique-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrail S3

[CloudWatch.1] Um filtro métrico de log e um alarme devem existir para uso do usuário “root”

[CloudWatch.4] Certifique-se de que exista um filtro de métrica de log e um alarme para alterações na política do IAM

[CloudWatch.5] Certifique-se de que exista um filtro métrico de log e um alarme para alterações de CloudTrail AWS Config duração

[CloudWatch.6] Certifique-se de que exista um filtro métrico de registro e um alarme para falhas de AWS Management Console autenticação

[CloudWatch.7] Certifique-se de que exista um filtro métrico de registro e um alarme para desativar ou excluir programadamente as chaves gerenciadas pelo cliente

[CloudWatch.8] Certifique-se de que exista um filtro métrico de log e um alarme para alterações na política do bucket do S3

[CloudWatch.9] Certifique-se de que exista um filtro métrico de registro e um alarme para alterações AWS Config de configuração

[CloudWatch.10] Certifique-se de que exista um filtro métrico de log e um alarme para alterações no grupo de segurança

[CloudWatch.11] Certifique-se de que exista um filtro métrico de registro e um alarme para alterações nas listas de controle de acesso à rede (NACL)

[CloudWatch.12] Certifique-se de que exista um filtro métrico de log e um alarme para alterações nos gateways de rede

[CloudWatch.13] Certifique-se de que exista um filtro métrico de log e um alarme para alterações na tabela de rotas

[CloudWatch.14] Certifique-se de que exista um filtro métrico de log e um alarme para alterações de VPC

[Config.1] AWS Config deve estar habilitado

[EC2.2] O grupo de segurança padrão da VPC não deve permitir o tráfego de entrada e saída

[EC2.6] O registro de fluxo de VPC deve ser ativado em todas as VPCs

[EC2.7] A criptografia padrão do EBS deve estar ativada

As ACLs de rede não devem permitir a entrada de 0.0.0.0/0 para a porta 22 ou porta 3389

[IAM.1] As políticas do não devem permitir privilégios administrativos completos "*"

[IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos

[IAM.4] A chave de acesso do usuário raiz do não deve existir

[IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console

[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz

[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz

1.9 Certifique-se de que a política de senha do IAM exija um comprimento mínimo de 14 ou mais

1.10 Certifique-se de que a política de senha do IAM impeça a reutilização de senhas

[IAM.18] Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support

As credenciais de usuário do IAM não utilizadas devem ser removidas

A rotação de AWS KMS teclas [KMS.4] deve estar ativada

[RDS.3] As instâncias de banco de dados do RDS devem ter a criptografia em repouso habilitada.

[S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas

[S3.5] Os buckets de uso geral do S3 devem exigir solicitações de uso de SSL

[S3.8] Os buckets de uso geral do S3 devem bloquear o acesso público

[S3.20] Os buckets de uso geral do S3 devem ter a exclusão de MFA habilitada

Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0

O Security Hub é compatível com a versão 1.2.0 do CIS AWS Foundations Benchmark.

O satisfez os requisitos de segurança do CIS Software Certification e recebeu a CIS Security Software Certification para as seguintes referências da CIS:

- Benchmark CIS para CIS AWS Foundations Benchmark, v1.2.0, Nível 1
- Benchmark CIS para CIS AWS Foundations Benchmark, v1.2.0, Nível 2

Controles que se aplicam ao CIS AWS Foundations Benchmark v1.2.0

[CloudTrail.1] CloudTrail deve ser habilitado e configurado com pelo menos uma trilha multirregional que inclua eventos de gerenciamento de leitura e gravação

[CloudTrail.2] CloudTrail deve ter a criptografia em repouso ativada

[CloudTrail.4] a validação do arquivo de CloudTrail log deve estar ativada

[CloudTrail.5] CloudTrail trilhas devem ser integradas com o Amazon CloudWatch Logs

[CloudTrail.6] Certifique-se de que o bucket do S3 usado para armazenar CloudTrail registros não esteja acessível ao público

[CloudTrail.7] Certifique-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrail S3

[CloudWatch.1] Um filtro métrico de log e um alarme devem existir para uso do usuário “root”

[CloudWatch.2] Certifique-se de que exista um filtro métrico de registro e um alarme para chamadas de API não autorizadas

[CloudWatch.3] Certifique-se de que exista um filtro métrico de registro e um alarme para o login do Management Console sem MFA

[CloudWatch.4] Certifique-se de que exista um filtro de métrica de log e um alarme para alterações na política do IAM

[CloudWatch.5] Certifique-se de que exista um filtro métrico de log e um alarme para alterações de CloudTrail AWS Config duração

[CloudWatch.6] Certifique-se de que exista um filtro métrico de registro e um alarme para falhas de AWS Management Console autenticação

[CloudWatch.7] Certifique-se de que exista um filtro métrico de registro e um alarme para desativar ou excluir programadamente as chaves gerenciadas pelo cliente

[CloudWatch.8] Certifique-se de que exista um filtro métrico de log e um alarme para alterações na política do bucket do S3

[CloudWatch.9] Certifique-se de que exista um filtro métrico de registro e um alarme para alterações AWS Config de configuração

[CloudWatch.10] Certifique-se de que exista um filtro métrico de log e um alarme para alterações no grupo de segurança

[CloudWatch.11] Certifique-se de que exista um filtro métrico de registro e um alarme para alterações nas listas de controle de acesso à rede (NACL)

[CloudWatch.12] Certifique-se de que exista um filtro métrico de log e um alarme para alterações nos gateways de rede

[CloudWatch.13] Certifique-se de que exista um filtro métrico de log e um alarme para alterações na tabela de rotas

[CloudWatch.14] Certifique-se de que exista um filtro métrico de log e um alarme para alterações de VPC

[Config.1] AWS Config deve estar habilitado

[EC2.2] O grupo de segurança padrão da VPC não deve permitir o tráfego de entrada e saída

[EC2.6] O registro de fluxo de VPC deve ser ativado em todas as VPCs

[EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22

[EC2.14] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 3389

[IAM.1] As políticas do não devem permitir privilégios administrativos completos "*"

[IAM.2] Os usuários do não devem ter políticas do IAM anexadas

[IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos

[IAM.4] A chave de acesso do usuário raiz do não deve existir

[IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console

[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz

As credenciais de usuário do IAM não utilizadas devem ser removidas

[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz

1.5 Certifique-se de que política de senha do IAM exija pelo menos uma letra maiúscula

1.6 Certifique-se de que política de senha do IAM exija pelo menos uma letra minúscula

1.7 Certifique-se de que política de senha do IAM exija pelo menos um símbolo

Certifique-se de que política de senha do IAM exija pelo menos um número

1.9 Certifique-se de que a política de senha do IAM exija um comprimento mínimo de 14 ou mais

1.10 Certifique-se de que a política de senha do IAM impeça a reutilização de senhas

1.11 Certifique-se de que a política de senha do IAM expire senhas em até 90 dias ou menos

[IAM.18] Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support

A rotação de AWS KMS teclas [KMS.4] deve estar ativada

Comparação de versões para o CIS AWS Foundations Benchmark

Esta seção resume as diferenças entre os benchmark v3.0.0, v1.4.0 e v1.2.0 do Center for Internet Security (CIS) AWS Foundations.

O Security Hub oferece suporte a cada uma dessas versões do CIS AWS Foundations Benchmark, mas recomendamos usar a v3.0.0 para se manter atualizado sobre as melhores práticas de segurança. Você pode ter várias versões do padrão ativadas ao mesmo tempo. Para ter mais informações, consulte Disabling or enabling a security standard (Desabilitar ou habilitar um padrão de segurança). Se você quiser atualizar para a v3.0.0, é melhor ativá-la antes de desativar uma versão mais antiga. Se você usa a integração do Security Hub com AWS Organizations para gerenciar

centralmente várias Contas da AWS e quiser habilitar em lote a v3.0.0 em todas as contas, poderá usar a configuração central.

Mapeamento de controles de acordo com os requisitos do CIS em cada versão

Entenda quais controles cada versão do CIS AWS Foundations Benchmark suporta.

Título e ID do controle	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[Conta.1] As informações de contato de segurança devem ser fornecidas para um Conta da AWS	1.2	1.2	1,18
[CloudTrail.1] CloudTrail deve ser habilitado e configurado com pelo menos uma trilha multirregional que inclua eventos de gerenciamento de leitura e gravação	3.1	3.1	2.1
[CloudTrail.1] CloudTrail deve ser habilitado e configurado com pelo menos uma trilha multirregional que inclua eventos de gerenciamento de leitura e gravação	3.1	3.1	2.1
[CloudTrail.2] CloudTrail deve ter a criptografia em repouso ativada	3.5	3.7	2.7
[CloudTrail.4] a validação do arquivo de CloudTrail log deve estar ativada	3.2	3.2	2.2
[CloudTrail.5] CloudTrail trilhas devem ser integradas com o Amazon CloudWatch Logs	Não suportado — o CIS removeu esse requisito	3.4	2.4
[CloudTrail.6] Certifique-se de que o bucket do S3 usado para armazenar	Não suportado — o CIS	3.3	2.3

Título e ID do controle	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
CloudTrail registros não esteja acessível ao público	removeu esse requisito		
[CloudTrail.7] Certifique-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrail S3	3.4	3.6	2.6
[CloudWatch.1] Um filtro métrico de log e um alarme devem existir para uso do usuário “root”	Não suportado — verificação manual	4.3	3.3
[CloudWatch.2] Certifique-se de que exista um filtro métrico de registro e um alarme para chamadas de API não autorizadas	Não suportado — verificação manual	Não suportado — verificação manual	3.1
[CloudWatch.3] Certifique-se de que exista um filtro métrico de registro e um alarme para o login do Management Console sem MFA	Não suportado — verificação manual	Não suportado — verificação manual	3.2
[CloudWatch.4] Certifique-se de que exista um filtro de métrica de log e um alarme para alterações na política do IAM	Não suportado — verificação manual	4.4	3.4
[CloudWatch.5] Certifique-se de que exista um filtro métrico de log e um alarme para alterações de CloudTrail AWS Config duração	Não suportado — verificação manual	4.5	3.5
[CloudWatch.6] Certifique-se de que exista um filtro métrico de registro e um alarme para falhas de AWS Management Console autenticação	Não suportado — verificação manual	4.6	3.6

Título e ID do controle	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[CloudWatch.7] Certifique-se de que exista um filtro métrico de registro e um alarme para desativar ou excluir programadamente as chaves gerenciadas pelo cliente	Não suportado — verificação manual	4.7	3.7
[CloudWatch.8] Certifique-se de que exista um filtro métrico de log e um alarme para alterações na política do bucket do S3	Não suportado — verificação manual	4.8	3.8
[CloudWatch.9] Certifique-se de que exista um filtro métrico de registro e um alarme para alterações AWS Config de configuração	Não suportado — verificação manual	4,9	3.9
[CloudWatch.10] Certifique-se de que exista um filtro métrico de log e um alarme para alterações no grupo de segurança	Não suportado — verificação manual	4.10	3.10
[CloudWatch.11] Certifique-se de que exista um filtro métrico de registro e um alarme para alterações nas listas de controle de acesso à rede (NACL)	Não suportado — verificação manual	4.11	3.11
[CloudWatch.12] Certifique-se de que exista um filtro métrico de log e um alarme para alterações nos gateways de rede	Não suportado — verificação manual	4.12	3.12
[CloudWatch.13] Certifique-se de que exista um filtro métrico de log e um alarme para alterações na tabela de rotas	Não suportado — verificação manual	4.13	3.13

Título e ID do controle	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[CloudWatch.14] Certifique-se de que exista um filtro métrico de log e um alarme para alterações de VPC	Não suportado — verificação manual	4.14	3.14
[Config.1] AWS Config deve estar habilitado	3.3	3.5	2,5
[EC2.2] O grupo de segurança padrão da VPC não deve permitir o tráfego de entrada e saída	5.4	5.3	4.3
[EC2.6] O registro de fluxo de VPC deve ser ativado em todas as VPCs	3.7	3.9	2.9
[EC2.7] A criptografia padrão do EBS deve estar ativada	2.2.1	2.2.1	Não suportado
As instâncias do EC2 devem usar o Instance Metadata Service Version 2 (IMDSv2)	5.6	Não suportado	Sem suporte
[EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22	Não suportado — substituído pelos requisitos 5.2 e 5.3	Não suportado — substituído pelos requisitos 5.2 e 5.3	4.1
[EC2.14] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 3389	Não suportado — substituído pelos requisitos 5.2 e 5.3	Não suportado — substituído pelos requisitos 5.2 e 5.3	4.2
As ACLs de rede não devem permitir a entrada de 0.0.0.0/0 para a porta 22 ou porta 3389	5.1	5.1	Não suportado

Título e ID do controle	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[EC2.53] Os grupos de segurança do EC2 não devem permitir a entrada de 0.0.0.0/0 nas portas de administração remota do servidor	5.2	Não suportado	Sem suporte
[EC2.54] Os grupos de segurança do EC2 não devem permitir a entrada de: :/0 nas portas de administração do servidor remoto	5.3	Não suportado	Sem suporte
[EFS.1] O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS	2.4.1	Não suportado	Não suportado
[IAM.1] As políticas do não devem permitir privilégios administrativos completos "*"	Sem suporte	1.16	1,22
[IAM.2] Os usuários do não devem ter políticas do IAM anexadas	1.15	Não suportado	1.16
[IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos	1.14	1.14	1.4
[IAM.4] A chave de acesso do usuário raiz do não deve existir	1.4	1.4	1.12
[IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console	1.10	1.10	1.2
[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz	1,6	1.6	1.14

Título e ID do controle	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
As credenciais de usuário do IAM não utilizadas devem ser removidas	Não suportado — veja As credenciais de usuário do IAM não utilizadas devem ser removidas em vez disso	Não suportado — veja As credenciais de usuário do IAM não utilizadas devem ser removidas em vez disso	1.3
[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz	1.5	1.5	1.13
1.5 Certifique-se de que política de senha do IAM exija pelo menos uma letra maiúscula	Não suportado — o CIS removeu esse requisito	Não suportado — o CIS removeu esse requisito	1.5
1.6 Certifique-se de que política de senha do IAM exija pelo menos uma letra minúscula	Não suportado — o CIS removeu esse requisito	Não suportado — o CIS removeu esse requisito	1.6
1.7 Certifique-se de que política de senha do IAM exija pelo menos um símbolo	Não suportado — o CIS removeu esse requisito	Não suportado — o CIS removeu esse requisito	1,7
Certifique-se de que política de senha do IAM exija pelo menos um número	Não suportado — o CIS removeu esse requisito	Não suportado — o CIS removeu esse requisito	1.8
1.9 Certifique-se de que a política de senha do IAM exija um comprimento mínimo de 14 ou mais	1.8	1.8	1.9

Título e ID do controle	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
1.10 Certifique-se de que a política de senha do IAM impeça a reutilização de senhas	1.9	1.9	1.10
1.11 Certifique-se de que a política de senha do IAM expire senhas em até 90 dias ou menos	Não suportado — o CIS removeu esse requisito	Não suportado — o CIS removeu esse requisito	1.11
[IAM.18] Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support	1.17	1.17	1.2
Evitar o uso do usuário raiz	Não suportado — o CIS removeu esse requisito	Não suportado — o CIS removeu esse requisito	1.1
As credenciais de usuário do IAM não utilizadas devem ser removidas	1.12	1.12	Não suportado — o CIS adicionou esse requisito em versões posteriores
[IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos	1,19	Não suportado — o CIS adicionou esse requisito em versões posteriores	Não suportado — o CIS adicionou esse requisito em versões posteriores

Título e ID do controle	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[IAM.27] As identidades do IAM não devem ter a política anexada AWSCloudShellFullAccess	1,22	Não suportado — o CIS adicionou esse requisito em versões posteriores	Não suportado — o CIS adicionou esse requisito em versões posteriores
[IAM.28] O analisador de acesso externo do IAM Access Analyzer deve estar ativado	1,20	Não suportado — o CIS adicionou esse requisito em versões posteriores	Não suportado — o CIS adicionou esse requisito em versões posteriores
A rotação de AWS KMS teclas [KMS.4] deve estar ativada	3.6	3.8	2.8
[Macie.1] O Amazon Macie deve estar ativado	Não suportado — verificação manual	Não suportado — verificação manual	Não suportado — verificação manual
[RDS.2] As instâncias de banco de dados do RDS devem proibir o acesso público, conforme determinado pela duração PubliclyAccessible AWS Config	2.3.3	Não suportado — o CIS adicionou esse requisito em versões posteriores	Não suportado — o CIS adicionou esse requisito em versões posteriores
[RDS.3] As instâncias de banco de dados do RDS devem ter a criptografia em repouso habilitada.	2.3.1	2.3.1	Não suportado — o CIS adicionou esse requisito em versões posteriores

Título e ID do controle	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[RDS.13] As atualizações automáticas de versões secundárias do RDS devem ser ativadas	2.3.2	Não suportado — o CIS adicionou esse requisito em versões posteriores	Não suportado — o CIS adicionou esse requisito em versões posteriores
[S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas	2.1.4	2.1.5	Não suportado — o CIS adicionou esse requisito em versões posteriores
[S3.5] Os buckets de uso geral do S3 devem exigir solicitações de uso de SSL	2.1.1	2.1.2	Não suportado — o CIS adicionou esse requisito em versões posteriores
[S3.8] Os buckets de uso geral do S3 devem bloquear o acesso público	2.1.4	2.1.5	Não suportado — o CIS adicionou esse requisito em versões posteriores
[S3.20] Os buckets de uso geral do S3 devem ter a exclusão de MFA habilitada	2.1.2	2.1.3	Não suportado — o CIS adicionou esse requisito em versões posteriores

Referência de ARNs para CIS Foundations AWS

Ao habilitar uma ou mais versões do CIS AWS Foundations Benchmark, você começará a receber descobertas no AWS Security Finding Format (ASFF). No ASFF, cada versão usa o seguinte Amazon Resource Name (ARN):

Referência do CIS AWS Foundations v3.0.0

```
arn:aws::securityhub:::standards/cis-aws-foundations-benchmark/v/3.0.0
```

Referência do CIS AWS Foundations v1.4.0

```
arn:aws::securityhub:::standards/cis-aws-foundations-benchmark/v/1.4.0
```

Referência do CIS AWS Foundations v1.2.0

```
arn:aws::securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

Você pode usar a GetEnabledStandardsoperação da API do Security Hub para descobrir o ARN de um padrão habilitado.

> **Note**
>
> Quando você habilita uma versão do CIS AWS Foundations Benchmark, o Security Hub pode levar até 18 horas para gerar descobertas para controles que usam a mesma regra AWS Config vinculada ao serviço dos controles habilitados em outros padrões habilitados. Para ter mais informações, consulte Programar a execução de verificações de segurança.

Os campos de localização serão diferentes se você ativar as descobertas de controle consolidadas. Para obter mais informações sobre essas diferenças, consulte Impacto da consolidação nos campos e valores do ASFF. Para obter os resultados do controle de amostras, consulteExemplo de descobertas de controle.

Requisitos do CIS que não são suportados no Security Hub

Conforme observado na tabela anterior, o Security Hub não suporta todos os requisitos do CIS em todas as versões do CIS Foundations AWS Benchmark. Muitos dos requisitos não suportados só podem ser avaliados manualmente por meio da análise do estado de seus AWS recursos.

Instituto Nacional de Padrões e Tecnologia (National Institute of Standards and Technology, NIST) SP 800-53 (Revisão 4)

O NIST SP 800-53 Rev. 5 é uma estrutura de segurança cibernética e conformidade desenvolvida pelo National Institute of Standards and Technology (NIST), uma agência que faz parte do Departamento de Comércio dos EUA. Essa estrutura de conformidade ajuda você a proteger a disponibilidade, a confidencialidade e a integridade de seus sistemas de informações e recursos essenciais. Agências e prestadores de serviços do governo federal dos EUA devem estar em conformidade com o NIST SP 800-53 para proteger seus sistemas, mas empresas privadas podem usá-la voluntariamente como uma estrutura orientadora para reduzir o risco de segurança cibernética.

O Security Hub fornece controles que suportam determinados requisitos do NIST SP 800-53. Esses controles são avaliados por meio de verificações de segurança automatizadas. Os controles do Security Hub não suportam os requisitos do NIST SP 800-53 que exigem verificações manuais. Além disso, os controles do Security Hub suportam apenas os requisitos automatizados do NIST SP 800-53, listados como requisitos relacionados nos detalhes de cada controle. Escolha um controle da lista a seguir para ver seus detalhes. No momento, os requisitos relacionados não mencionados nos detalhes do controle não são suportados pelo Security Hub.

Ao contrário de outras estruturas, o NIST SP 800-53 não é prescritivo sobre como seus requisitos devem ser avaliados. Em vez disso, a estrutura fornece diretrizes, e os controles NIST SP 800-53 do Security Hub representam a compreensão do serviço sobre elas.

Se você usar a integração do Security Hub AWS Organizations para gerenciar centralmente várias contas e quiser habilitar em lote o NIST SP 800-53 em todas elas, poderá executar um script de várias contas do Security Hub a partir da conta do administrador.

Para obter mais informações sobre o NIST SP 800-53 Rev. 5, consulte o NIST Computer Security Resource Center.

Controles que se aplicam ao NIST SP 800-53 Rev. 5

[Conta.1] As informações de contato de segurança devem ser fornecidas para um Conta da AWS

[A conta.2] Contas da AWS deve fazer parte de uma organização AWS Organizations

Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado

[ApiGateway.1] O REST do API Gateway WebSocket e o registro de execução da API devem estar habilitados

Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end

Os estágios da API REST de Gateway devem ter o rastreamento AWS X-Ray habilitado.

O API Gateway deve ser associado a uma WAF Web ACL

Os dados do cache da API REST de Gateway devem ser criptografados em repouso

As rotas do API de Gateway devem especificar um tipo de autorização

O registro de acesso deve ser configurado para os estágios V2 do API de Gateway

[AppSync.5] As APIs AWS AppSync do GraphQL não devem ser autenticadas com chaves de API

[AutoScaling.1] Grupos de Auto Scaling associados a um balanceador de carga devem usar verificações de integridade do ELB

[AutoScaling.2] O grupo Amazon EC2 Auto Scaling deve abranger várias zonas de disponibilidade

[AutoScaling.3] As configurações de lançamento de grupos do Auto Scaling devem configurar as instâncias do EC2 para exigir o Instance Metadata Service Version 2 (IMDSv2)

As instâncias do Amazon EC2 lançadas usando as configurações de execução em grupo do Auto Scaling não devem ter endereços IP públicos

[AutoScaling.6] Os grupos de Auto Scaling devem usar vários tipos de instância em várias zonas de disponibilidade

[AutoScaling.9] Os grupos do Amazon EC2 Auto Scaling devem usar os modelos de lançamento do Amazon EC2

[Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso

[CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado

[CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito

[CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado

[CloudFront.5] CloudFront as distribuições devem ter o registro ativado

[CloudFront.6] as CloudFront distribuições devem ter o WAF ativado

[CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados

[CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS

[CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas

[CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas

[CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3

[CloudTrail.1] CloudTrail deve ser habilitado e configurado com pelo menos uma trilha multirregional que inclua eventos de gerenciamento de leitura e gravação

[CloudTrail.2] CloudTrail deve ter a criptografia em repouso ativada

[CloudTrail.4] a validação do arquivo de CloudTrail log deve estar ativada

[CloudTrail.5] CloudTrail trilhas devem ser integradas com o Amazon CloudWatch Logs

[CloudWatch.15] CloudWatch os alarmes devem ter ações especificadas configuradas

[CloudWatch.16] os grupos de CloudWatch registros devem ser mantidos por um período de tempo especificado

[CloudWatch.17] ações de CloudWatch alarme devem ser ativadas

[CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais

[CodeBuild.2] as variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado

[CodeBuild.3] Os registros do CodeBuild S3 devem ser criptografados

[CodeBuild.4] ambientes de CodeBuild projeto devem ter uma duração de registro AWS Config

[Config.1] AWS Config deve estar habilitado

[DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso

As instâncias de replicação do PCI.DMS.1 Database Migration Service não devem ser públicas

As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada

As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado

As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado

Os endpoints do DMS devem usar SSL

[DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada

[DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado

[DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado

Os clusters do Amazon DocumentDB devem ser criptografados em repouso

Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado

Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos

[DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch

Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada

As tabelas do DynamoDB devem escalar automaticamente a capacidade de acordo com a demanda

[DynamoDB.2] As tabelas do DynamoDB devem ter a recuperação ativada point-in-time

Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso

As tabelas do DynamoDB devem estar presentes em um plano de backup

[DynamoDB.6] As tabelas do DynamoDB devem ter a proteção contra exclusão habilitada

[DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito

[PCI.EC2.1] Os instantâneos do Amazon EBS não devem ser restauráveis publicamente

[EC2.2] O grupo de segurança padrão da VPC não deve permitir o tráfego de entrada e saída

[EC2.3] Os volumes anexados do Amazon EBS devem ser criptografados em repouso.

As instâncias EC2 interrompidas devem ser removidas após um período de tempo especificado

[EC2.6] O registro de fluxo de VPC deve ser ativado em todas as VPCs

[EC2.7] A criptografia padrão do EBS deve estar ativada

As instâncias do EC2 devem usar o Instance Metadata Service Version 2 (IMDSv2)

As instâncias do Amazon EC2 não devem ter um endereço IPv4 público

O Amazon EC2 deve ser configurado para usar endpoints da VPC criados para o serviço Amazon EC2

[PCI.EC2.4] Os EIPs do EC2 não utilizados devem ser removidos

[EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22

As sub-redes do Amazon EC2 não devem atribuir automaticamente endereços IP públicos

As listas de controle de acesso à rede não utilizadas devem ser removidas

As instâncias do Amazon EC2 não devem usar vários ENIs

Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas

Grupos de segurança não devem permitir acesso irrestrito a portas com alto risco

[EC2.20] Ambos os túneis VPN para uma conexão VPN Site-to-Site devem estar ativos AWS

As ACLs de rede não devem permitir a entrada de 0.0.0.0/0 para a porta 22 ou porta 3389

Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC

Os tipos de instância paravirtual do Amazon EC2 não devem ser usados

Os modelos de lançamento do Amazon EC2 não devem atribuir IPs públicos às interfaces de rede

[EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup

[EC2.51] Os endpoints da Client VPN do EC2 devem ter o registro em log de conexão do cliente habilitado

Os repositórios privados do ECR devem ter a digitalização de imagens configurada

[ECR.2] Os repositórios privados do ECR devem ter a imutabilidade da tag configurada

Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada

As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário.

Os serviços do ECS não devem ter endereços IP públicos atribuídos a eles automaticamente

As definições de tarefas do ECS não devem compartilhar o namespace do processo do host

Os contêineres ECS devem ser executados sem privilégios

Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz

Os segredos não devem ser passados como variáveis de ambiente do contêiner

As definições de tarefas do ECS devem ter uma configuração de registro em log

Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate

Os clusters do ECS devem usar Container Insights

[EFS.1] O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS

[EFS.2] Os volumes do Amazon EFS devem estar em planos de backup

Os pontos de acesso do EFS devem impor um diretório raiz

Os pontos de acesso do EFS devem impor uma identidade de usuário

[EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública

Os endpoints do cluster EKS não devem ser acessíveis ao público

Os clusters EKS devem ser executados em uma versão compatível do Kubernetes

[EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes

[EKS.8] Os clusters do EKS devem ter o registro em log de auditoria habilitado

[ElastiCache.1] Os clusters ElastiCache Redis devem ter o backup automático ativado

[ElastiCache.2] ElastiCache para clusters de cache Redis deve ter a atualização automática de versão secundária habilitada

[ElastiCache.3] ElastiCache para grupos de replicação do Redis, o failover automático deve estar ativado

[ElastiCache.4] ElastiCache para Redis, os grupos de replicação devem ser criptografados em repouso

[ElastiCache.5] ElastiCache para Redis, os grupos de replicação devem ser criptografados em trânsito

[ElastiCache.6] ElastiCache para grupos de replicação do Redis antes da versão 6.0 deve usar o Redis AUTH

[ElastiCache.7] os ElastiCache clusters não devem usar o grupo de sub-rede padrão

[ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de integridade aprimorados habilitados

[ElasticBeanstalk.2] As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas

[ELBv2.1] O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS

[ELB.2] Os balanceadores de carga clássicos com ouvintes SSL/HTTPS devem usar um certificado fornecido pelo AWS Certificate Manager

Os receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS

O Application Load Balancer deve ser configurado para eliminar cabeçalhos http

O registro em log do Classic Load Balancer e Application Load Balancer deve estar ativado

[ELB.6] Os balanceadores de carga de aplicativos, gateways e redes devem ter a proteção contra exclusão ativada

Os Classic Load Balancers devem ter a drenagem da conexão ativada

[ELB.8] Os balanceadores de carga clássicos com ouvintes SSL devem usar uma política de segurança predefinida que tenha uma duração forte AWS Config

Os Classic Load Balancers devem ter o balanceador de carga entre zonas habilitado

Verifica se o Classic Load Balancer abrange várias zonas de disponibilidade (AZs).

O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso

Balanceadores de carga de aplicações, redes e gateways não abrangem várias zonas de disponibilidade

O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso

[ELB.16] Os balanceadores de carga de aplicativos devem ser associados a uma ACL da web AWS WAF

[EMR.1] Os nós primários do cluster do Amazon EMR não devem ter endereços IP públicos

[EMR.2] A configuração de bloqueio de acesso público do Amazon EMR deve estar habilitada

[ES.1] Os domínios do devem ter a criptografia em repouso habilitada.

[ES.2] Os domínios do Elasticsearch não devem ser publicamente acessíveis

Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós

[ES.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado

Os domínios do Elasticsearch devem ter o registro em log de auditoria ativado

Os domínios do Elasticsearch devem ter pelo menos três nós de dados

Os domínios do Elasticsearch devem ser configurados com pelo menos três nós principais dedicados

[ES.8] As conexões com os domínios do Elasticsearch devem ser criptografadas usando a política de segurança TLS mais recente

[EventBridge.3] os ônibus de eventos EventBridge personalizados devem ter uma política baseada em recursos anexada

[EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada

[FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.

[FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups

[GuardDuty.1] GuardDuty deve ser ativado

[IAM.1] As políticas do não devem permitir privilégios administrativos completos "*"

[IAM.2] Os usuários do não devem ter políticas do IAM anexadas

[IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos

[IAM.4] A chave de acesso do usuário raiz do não deve existir

[IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console

[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz

[IAM.7] As políticas de senha para usuários do IAM devem ter configurações fortes

As credenciais de usuário do IAM não utilizadas devem ser removidas

[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz

[PCI.IAM.6] A MFA deve estar habilitada para todos os usuários do

As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.

Os fluxos do Kinesis devem ser criptografados em repouso

As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS

As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS

[KMS.3] não AWS KMS keys deve ser excluído acidentalmente

A rotação de AWS KMS teclas [KMS.4] deve estar ativada

[PCI.lambda.1] As funções do devem proibir o acesso público

[Lambda.2] As funções do devem usar os tempos de execução mais recentes

[PCI.Lambda.2] As funções do Lambda devem estar em uma VPC

[Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade

[Macie.1] O Amazon Macie deve estar ativado

[Macie.2] A descoberta automatizada de dados confidenciais do Macie deve ser ativada

Os clusters MSK devem ser criptografados em trânsito entre os nós do agente

[MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado

[MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch

[MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada

Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera

Os agentes do RabbitMQ devem usar o modo de implantação de cluster

Os clusters de banco de dados Neptune devem ser criptografados em repouso

[Neptune.2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch

Os instantâneos do cluster de banco de dados Neptune não devem ser públicos

[Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada

Os clusters de banco de dados Neptune devem ter backups automatizados habilitados

Os clusters de banco de dados Neptune devem ser criptografados em repouso

[Neptune.7] Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada

Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos

[Neptune.9] Os clusters de banco de dados do Neptune devem ser implantados em várias zonas de disponibilidade

[NetworkFirewall.1] Os firewalls do Network Firewall devem ser implantados em várias zonas de disponibilidade

[NetworkFirewall.2] O registro do Firewall de Rede deve estar ativado

[NetworkFirewall.3] As políticas de Firewall de Rede devem ter pelo menos um grupo de regras associado

[NetworkFirewall.4] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar pacotes completos

[NetworkFirewall.5] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar para pacotes fragmentados

[NetworkFirewall.6] O grupo de regras do Stateless Network Firewall não deve estar vazio

[NetworkFirewall.9] Os firewalls do Firewall de Rede devem ter a proteção contra exclusão ativada

Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada

Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público

Os OpenSearch domínios [Opensearch.3] devem criptografar os dados enviados entre os nós

O registro de erros de OpenSearch domínio [Opensearch.4] nos CloudWatch registros deve estar ativado

Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado

Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados

Os OpenSearch domínios [Opensearch.7] devem ter um controle de acesso refinado ativado

[Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente

Os OpenSearch domínios [Opensearch.10] devem ter a atualização de software mais recente instalada

Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados

[PCA.1] a autoridade de certificação AWS Private CA raiz deve ser desativada

[RDS.1] Os instantâneos do RDS devem ser privados

[RDS.2] As instâncias de banco de dados do RDS devem proibir o acesso público, conforme determinado pela duração PubliclyAccessible AWS Config

[RDS.3] As instâncias de banco de dados do RDS devem ter a criptografia em repouso habilitada.

Os instantâneos do cluster do RDS e os instantâneos do banco de dados devem ser criptografados em repouso

As instâncias de banco de dados do RDS devem ser configuradas com várias zonas de disponibilidade

O monitoramento aprimorado deve ser configurado para instâncias de banco de dados do RDS

[RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada

[RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada

[RDS.9] As instâncias de banco de dados do RDS devem publicar registros no Logs CloudWatch

A autenticação do IAM deve ser configurada para instâncias do RDS

As instâncias do RDS devem ter backups automáticos habilitados

A autenticação do IAM deve ser configurada para instâncias do RDS

[RDS.13] As atualizações automáticas de versões secundárias do RDS devem ser ativadas

[RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado

[RDS.15] Os clusters de banco de dados do RDS devem ser configurados para várias zonas de disponibilidade

Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos

As instâncias de banco de dados do RDS devem ser configuradas para copiar tags para instantâneos

As instâncias do RDS devem ser implantadas em uma VPC

As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de cluster

As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de cluster

Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de parâmetros do banco de dados

Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de parâmetros do banco de dados

As instâncias do RDS não devem usar uma porta padrão do mecanismo de banco de dados

Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado

Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado

As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup

Os clusters de banco de dados Neptune devem ser criptografados em repouso

[RDS.34] Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch

Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada

[PCI.Redshift.1] Os clusters do devem proibir o acesso público

As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito

Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados

Os clusters do Amazon Redshift devem ter o registro de auditoria ativado

O Amazon Redshift deve ter as atualizações automáticas para as versões principais habilitadas

Os clusters do Redshift devem usar roteamento de VPC aprimorado

Os clusters do Amazon Redshift não devem usar o nome de usuário Admin padrão

[Redshift.9] Os clusters do Redshift não devem usar o nome do banco de dados padrão

[Redshift.10] Os clusters do Redshift devem ser criptografados em repouso

As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS

[S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas

[S3.2] Os buckets de uso geral do S3 devem bloquear o acesso público de leitura

[S3.3] Os buckets de uso geral do S3 devem bloquear o acesso público de gravação

[S3.5] Os buckets de uso geral do S3 devem exigir solicitações de uso de SSL

[S3.6] As políticas de bucket de uso geral do S3 devem restringir o acesso a outros Contas da AWS

[S3.7] Os buckets de uso geral do S3 devem usar a replicação entre regiões

[S3.8] Os buckets de uso geral do S3 devem bloquear o acesso público

[S3.9] Os buckets de uso geral do S3 devem ter o registro de acesso ao servidor ativado

[S3.10] Os buckets de uso geral do S3 com controle de versão ativado devem ter configurações de ciclo de vida

[S3.11] Os buckets de uso geral do S3 devem ter as notificações de eventos ativadas

[S3.12] As ACLs não devem ser usadas para gerenciar o acesso do usuário aos buckets de uso geral do S3

[S3.13] Os buckets de uso geral do S3 devem ter configurações de ciclo de vida

[S3.14] Os buckets de uso geral do S3 devem ter o controle de versão ativado

[S3.15] Os buckets de uso geral do S3 devem ter o Object Lock ativado

[S3.17] Os buckets de uso geral do S3 devem ser criptografados em repouso com AWS KMS keys

[S3.19] Os pontos de acesso do S3 devem ter configurações de bloqueio do acesso público habilitadas

[S3.20] Os buckets de uso geral do S3 devem ter a exclusão de MFA habilitada

[SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet

[SageMaker.2] as instâncias do SageMaker notebook devem ser iniciadas em uma VPC personalizada

[SageMaker.3] Os usuários não devem ter acesso root às instâncias do SageMaker notebook

[SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1

[SecretsManager.1] Os segredos do Secrets Manager devem ter a rotação automática ativada

[SecretsManager.2] Os segredos do Secrets Manager configurados com rotação automática devem girar com sucesso

[SecretsManager.3] Remover segredos não utilizados do Secrets Manager

[SecretsManager.4] Os segredos do Secrets Manager devem ser alternados dentro de um determinado número de dias

[ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS

[SNS.1] Os tópicos do SNS devem ser criptografados em repouso usando AWS KMS

As filas do Amazon SQS devem ser criptografadas em repouso

[SSM.1] As instâncias do Amazon EC2 devem ser gerenciadas por AWS Systems Manager

[PCI.SSM.1] As instâncias do Amazon EC2 gerenciadas pelo devem ter um status de conformidade de patch de COMPLIANT (Em conformidade) após a instalação do patch

PCI.SSM.2 As instâncias de Amazon EC2 gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL

Os documentos SSM não devem ser públicos

[Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints

[WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado

[WAF.2] As regras regionais AWS WAF clássicas devem ter pelo menos uma condição

[WAF.3] Os grupos de regras regionais AWS WAF clássicos devem ter pelo menos uma regra

[WAF.4] As ACLs regionais AWS WAF clássicas da web devem ter pelo menos uma regra ou grupo de regras

[WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição

[WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra

[WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

[WAF.10] as ACLs AWS WAF da web devem ter pelo menos uma regra ou grupo de regras

[WAF.11] O registro de ACL AWS WAF da web deve estar ativado

As AWS WAF regras [WAF.12] devem ter métricas habilitadas CloudWatch

Padrão de segurança de dados do setor de cartão de pagamento (PCI DSS – Payment Card Industry Data Security Standard)

O Payment Card Industry Data Security Standard (PCI DSS) no Security Hub fornece um conjunto de melhores práticas de segurança da AWS para o tratamento de dados do titular do cartão. É possível usar esse padrão para descobrir vulnerabilidades de segurança em recursos que lidam com dados de titulares de cartões. No momento, o tem como escopo os controles no nível da conta. É recomendável habilitar esses controles em todas as contas com recursos que armazenam, processam e/ou transmitem dados do titular do cartão.

Esse padrão foi validado pela AWS Security Assurance Services LLC (AWS SAS), que é uma equipe de avaliadores de segurança qualificados (QSAs) certificados para fornecer orientação sobre o PCI DSS e avaliações pelo PCI DSS Security Standards Council (PCI SSC). AWS O SAS confirmou que as verificações automatizadas podem ajudar o cliente a se preparar para uma avaliação do PCI DSS.

Esta página lista IDs e títulos de controle de segurança. Nas regiões AWS GovCloud (US) Region e na China, IDs e títulos de controle específicos do padrão são usados. A tabela a seguir mostra o mapeamento de IDs e títulos de controle de segurança para IDs e títulos de controle específicos do padrão.

Controles que se aplicam ao PCI DSS

[AutoScaling.1] Grupos de Auto Scaling associados a um balanceador de carga devem usar verificações de integridade do ELB

[CloudTrail.2] CloudTrail deve ter a criptografia em repouso ativada

[CloudTrail.3] Pelo menos uma CloudTrail trilha deve ser ativada

[CloudTrail.4] a validação do arquivo de CloudTrail log deve estar ativada

[CloudTrail.5] CloudTrail trilhas devem ser integradas com o Amazon CloudWatch Logs

[CloudWatch.1] Um filtro métrico de log e um alarme devem existir para uso do usuário “root”

[CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais

[CodeBuild.2] as variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado

[Config.1] AWS Config deve estar habilitado

As instâncias de replicação do PCI.DMS.1 Database Migration Service não devem ser públicas

[PCI.EC2.1] Os instantâneos do Amazon EBS não devem ser restauráveis publicamente

[EC2.2] O grupo de segurança padrão da VPC não deve permitir o tráfego de entrada e saída

[EC2.6] O registro de fluxo de VPC deve ser ativado em todas as VPCs

[PCI.EC2.4] Os EIPs do EC2 não utilizados devem ser removidos

[EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22

[ELBv2.1] O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS

[ES.1] Os domínios do devem ter a criptografia em repouso habilitada.

[ES.2] Os domínios do Elasticsearch não devem ser publicamente acessíveis

[GuardDuty.1] GuardDuty deve ser ativado

[IAM.1] As políticas do não devem permitir privilégios administrativos completos "*"

[IAM.2] Os usuários do não devem ter políticas do IAM anexadas

[IAM.4] A chave de acesso do usuário raiz do não deve existir

[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz

As credenciais de usuário do IAM não utilizadas devem ser removidas

[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz

[IAM.10] As políticas de senha para usuários do IAM devem ter durações fortes AWS Config

[PCI.IAM.6] A MFA deve estar habilitada para todos os usuários do

A rotação de AWS KMS teclas [KMS.4] deve estar ativada

[PCI.lambda.1] As funções do devem proibir o acesso público

[PCI.Lambda.2] As funções do Lambda devem estar em uma VPC

Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada

Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público

[RDS.1] Os instantâneos do RDS devem ser privados

[RDS.2] As instâncias de banco de dados do RDS devem proibir o acesso público, conforme determinado pela duração PubliclyAccessible AWS Config

[PCI.Redshift.1] Os clusters do devem proibir o acesso público

[S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas

[S3.2] Os buckets de uso geral do S3 devem bloquear o acesso público de leitura

[S3.3] Os buckets de uso geral do S3 devem bloquear o acesso público de gravação

[S3.5] Os buckets de uso geral do S3 devem exigir solicitações de uso de SSL

[S3.7] Os buckets de uso geral do S3 devem usar a replicação entre regiões

[SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet

[SSM.1] As instâncias do Amazon EC2 devem ser gerenciadas por AWS Systems Manager

[PCI.SSM.1] As instâncias do Amazon EC2 gerenciadas pelo devem ter um status de conformidade de patch de COMPLIANT (Em conformidade) após a instalação do patch

PCI.SSM.2 As instâncias de Amazon EC2 gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL

AWS Padrão de marcação de recursos

Esta seção fornece informações sobre o Padrão de Marcação de AWS Recursos.

> **Note**
>
> O Padrão AWS de Etiquetagem de Recursos não está disponível no Oeste do Canadá (Calgary), China e. AWS GovCloud (US)

O que é o padrão AWS de marcação de recursos?

As tags são pares de chaves e valores que atuam como metadados para organizar seus AWS recursos. Com a maioria dos AWS recursos, você tem a opção de adicionar tags ao criar o recurso ou após a criação. Exemplos de recursos incluem uma CloudFront distribuição da Amazon, uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou uma entrada secreta. AWS Secrets Manager

As tags podem ajudar você a gerenciar, identificar, organizar, pesquisar e filtrar recursos.

Cada tag tem duas partes:

- Uma chave de tag (por exemplo ,`CostCenter`, `Environment` ou `Project`). Chaves de tag fazem distinção entre maiúsculas e minúsculas.
- Um valor de tag (por exemplo, `111122223333` ou`Production`). Como chaves de tag, os valores das tags diferenciam maiúsculas de minúsculas.

Você pode usar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios.

Para obter instruções sobre como adicionar tags aos AWS recursos, consulte Como adicionar tags ao seu AWS recurso no Guia do Usuário do AWS Security Hub.

O AWS Resource Tagging Standard, desenvolvido pelo AWS Security Hub, ajuda você a identificar rapidamente se faltam chaves de tag em algum de seus AWS recursos. Você pode personalizar o `requiredTagKeys` parâmetro para especificar chaves de tag específicas que os controles verificam. Se tags específicas não forem fornecidas, os controles apenas verificarão a existência de pelo menos uma chave de tag.

Ao habilitar o AWS Resource Tagging Standard, você começará a receber descobertas no AWS Security Finding Format (ASFF).

> **Note**
>
> Quando você ativa o AWS Resource Tagging Standard, o Security Hub pode levar até 18 horas para gerar descobertas para controles que usam a mesma regra AWS Config vinculada ao serviço dos controles habilitados em outros padrões habilitados. Para ter mais informações, consulte Programar a execução de verificações de segurança.

Esse padrão tem o seguinte nome de recurso da Amazon (ARN):.
`arn:aws:securityhub:region::standards/aws-resource-tagging-standard/v/1.0.0`

Você também pode usar a GetEnabledStandardsoperação da API do Security Hub para descobrir o ARN de um padrão habilitado.

Controles no padrão AWS de marcação de recursos

O Padrão AWS de Marcação de Recursos inclui os seguintes controles. Selecione um controle para ver uma descrição detalhada dele.

- [ACM.3] Os certificados ACM devem ser marcados
- [AppSync.4] As APIs AWS AppSync do GraphQL devem ser marcadas
- [Athena.2] Os catálogos de dados do Athena devem ser marcados
- [Athena.3] Os grupos de trabalho do Athena devem ser marcados
- [AutoScaling.10] Os grupos do EC2 Auto Scaling devem ser marcados
- [Backup.2] os pontos de AWS Backup recuperação devem ser marcados
- [Backup.3] os AWS Backup cofres devem ser marcados
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [Backup.5] os planos de AWS Backup backup devem ser marcados
- [CloudFormation.2] as CloudFormation pilhas devem ser marcadas
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CloudTrail.9] CloudTrail trilhas devem ser marcadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [Detetive.1] Os gráficos do comportamento do detetive devem ser marcados
- [DMS.2] Os certificados DMS devem ser marcados
- [DMS.3] As assinaturas de eventos do DMS devem ser marcadas
- [DMS.4] As instâncias de replicação do DMS devem ser marcadas
- [DMS.5] Os grupos de sub-redes de replicação do DMS devem ser marcados
- [DynamoDB.5] As tabelas do DynamoDB devem ser marcadas
- [EC2.33] Os anexos do gateway de trânsito EC2 devem ser marcados
- [EC2.34] As tabelas de rotas do gateway de trânsito EC2 devem ser marcadas

- [EC2.35] As interfaces de rede EC2 devem ser marcadas
- [EC2.36] Os gateways de clientes do EC2 devem ser marcados
- [EC2.37] Os endereços IP elásticos do EC2 devem ser marcados
- [EC2.38] As instâncias do EC2 devem ser marcadas
- [EC2.39] Os gateways de internet EC2 devem ser marcados
- [EC2.40] Os gateways NAT EC2 devem ser marcados
- [EC2.41] As ACLs de rede EC2 devem ser marcadas
- [EC2.42] As tabelas de rotas do EC2 devem ser marcadas
- [EC2.43] Grupos de segurança do EC2 devem ser marcados
- [EC2.44] As sub-redes do EC2 devem ser marcadas
- [EC2.45] Os volumes do EC2 devem ser marcados
- [EC2.46] Amazon VPCs devem ser marcadas
- [EC2.47] Os serviços de endpoint da Amazon VPC devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.49] As conexões de emparelhamento da Amazon VPC devem ser marcadas
- [EC2.50] Os gateways de VPN EC2 devem ser marcados
- [EC2.52] Os gateways de trânsito do EC2 devem ser marcados
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [ECS.13] Os serviços do ECS devem ser marcados
- [ECS.14] Os clusters ECS devem ser marcados
- [ECS.15] As definições de tarefas do ECS devem ser marcadas
- [EFS.5] Os pontos de acesso do EFS devem ser marcados
- [EKS.6] Os clusters EKS devem ser marcados
- [EKS.7] As configurações do provedor de identidade EKS devem ser marcadas
- [ES.9] Os domínios do Elasticsearch devem ser marcados
- [EventBridge.2] ônibus de EventBridge eventos devem ser etiquetados
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- Os AWS Glue trabalhos [Glue.1] devem ser marcados

- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] Os GuardDuty IPsets devem ser marcados
- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [IAM.23] Os analisadores do IAM Access Analyzer devem ser marcados
- [IAM.24] As funções do IAM devem ser marcadas
- [IAM.25] Os usuários do IAM devem ser marcados
- [IoT.1] perfis de AWS IoT Core segurança devem ser marcados
- [IoT.2] as ações de AWS IoT Core mitigação devem ser marcadas
- [IoT.3] as AWS IoT Core dimensões devem ser marcadas
- [IoT.4] os AWS IoT Core autorizadores devem ser marcados
- [IoT.5] aliases de AWS IoT Core função devem ser marcados
- As AWS IoT Core políticas [IoT.6] devem ser marcadas
- [Kinesis.2] Os streams do Kinesis devem ser marcados
- [Lambda.6] As funções Lambda devem ser marcadas
- [MQ.4] Os corretores do Amazon MQ devem ser marcados
- [NetworkFirewall.7] Os firewalls do Firewall de Rede devem ser marcados
- [NetworkFirewall.8] As políticas de firewall do Network Firewall devem ser marcadas
- Os OpenSearch domínios [Opensearch.9] devem ser marcados
- [RDS.28] Os clusters de banco de dados do RDS devem ser marcados
- [RDS.29] Os instantâneos do cluster de banco de dados do RDS devem ser marcados
- [RDS.30] As instâncias de banco de dados do RDS devem ser marcadas
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [RDS.32] Os instantâneos do banco de dados do RDS devem ser marcados
- [RDS.33] Os grupos de sub-redes do banco de dados do RDS devem ser marcados
- [Redshift.11] Os clusters do Redshift devem ser marcados
- [Redshift.12] As assinaturas de notificação de eventos do Redshift devem ser marcadas
- [Redshift.13] Os instantâneos do cluster do Redshift devem ser marcados
- [Redshift.14] Os grupos de sub-redes do cluster Redshift devem ser marcados
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas

- [SecretsManager.5] Os segredos do Secrets Manager devem ser marcados
- [SES.1] As listas de contatos do SES devem ser marcadas
- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [SNS.3] Os tópicos do SNS devem ser marcados
- [SQS.2] As filas SQS devem ser marcadas
- [StepFunctions.2] As atividades do Step Functions devem ser marcadas
- Os AWS Transfer Family fluxos de trabalho [Transfer.1] devem ser marcados

Padrões gerenciados por serviços

Um padrão gerenciado por serviços é um padrão de segurança gerenciado por outra pessoa AWS service (Serviço da AWS) . Por exemplo, Padrão gerenciado por serviços: AWS Control Toweré um padrão gerenciado por serviços que gerencia. AWS Control Tower Um padrão gerenciado por serviços difere de um padrão de segurança que o AWS Security Hub gerencia das seguintes maneiras:

- Criação e exclusão de padrões — Você cria e exclui um padrão gerenciado por serviços com o console ou a API do serviço de gerenciamento, ou com o AWS CLI. Até que você crie o padrão no serviço de gerenciamento de uma dessas formas, o padrão não aparece no console do Security Hub e não pode ser acessado pela API do Security Hub ou AWS CLI.
- Sem ativação automática dos controles — Quando você cria um padrão gerenciado pelo serviço, o Security Hub e o serviço de gerenciamento não ativam automaticamente os controles que se aplicam ao padrão. Além disso, quando o Security Hub lança novos controles para o padrão, eles não são ativados automaticamente. Isso é um desvio dos padrões que o Security Hub gerencia. Para obter mais informações sobre a maneira usual de configurar controles no Security Hub, consulte Visualizando e gerenciando padrões de segurança.
- Ativar e desativar controles — Recomendamos ativar e desativar os controles no serviço de gerenciamento para evitar desvios.
- Disponibilidade de controles — O serviço de gerenciamento escolhe quais controles estão disponíveis como parte do padrão gerenciado por serviços. Os controles disponíveis podem incluir todos ou um subconjunto dos controles existentes do Security Hub.

Depois que o serviço de gerenciamento criar o padrão gerenciado pelo serviço e disponibilizar os controles para ele, será possível acessar suas descobertas de controle, status de controle e

pontuação de segurança padrão no console do Security Hub, na API do Security Hub ou AWS CLI Algumas ou todas essas informações também podem estar disponíveis no serviço de gerenciamento.

Selecione um padrão gerenciado por serviços na lista a seguir para ver mais detalhes sobre ele.

Padrões gerenciados por serviços

- Padrão gerenciado por serviços: AWS Control Tower

Padrão gerenciado por serviços: AWS Control Tower

Esta seção fornece informações sobre o Service-Managed Standard:. AWS Control Tower

O que é o Service-Managed Standard:? AWS Control Tower

Esse padrão foi desenvolvido para usuários do AWS Security Hub AWS Control Tower e. Ele permite que você configure os controles proativos AWS Control Tower junto com os controles de detetive do Security Hub no AWS Control Tower serviço.

Os controles proativos ajudam a garantir que você Contas da AWS mantenha a conformidade, pois sinalizam ações que podem levar a violações de políticas ou configurações incorretas. Os controles de detetive detectam a não conformidade de recursos (por exemplo, configurações incorretas) em sua Contas da AWS. Ao habilitar controles proativos e detectivos para seu AWS ambiente, você pode aprimorar sua postura de segurança em diferentes estágios de desenvolvimento.

> **Tip**
>
> Os padrões gerenciados por serviços diferem dos padrões gerenciados pelo AWS Security Hub. Por exemplo, você deve criar e excluir um padrão gerenciado por serviços no serviço de gerenciamento. Para ter mais informações, consulte Padrões gerenciados por serviços.

No console e na API do Security Hub, você pode ver o Service-Managed Standard: AWS Control Tower junto com outros padrões do Security Hub.

Criando o padrão

Esse padrão estará disponível somente se você criar o padrão em AWS Control Tower. AWS Control Tower cria o padrão quando você ativa pela primeira vez um controle aplicável usando um dos seguintes métodos:

- AWS Control Tower console
- AWS Control Tower API (chame a `EnableControl`API)
- AWS CLI (execute o `enable-control`comando)

Os controles do Security Hub são identificados no AWS Control Tower console como SH. ***`ControlID`*** (por exemplo, SH. CodeBuild.1).

Ao criar o padrão, se você ainda não tiver habilitado o Security Hub, AWS Control Tower também habilita o Security Hub para você.

Se você não tiver configurado AWS Control Tower, não poderá visualizar ou acessar esse padrão no console do Security Hub, na API do Security Hub ou AWS CLI. Mesmo que você tenha configurado AWS Control Tower, não poderá visualizar ou acessar esse padrão no Security Hub sem primeiro criar o padrão AWS Control Tower usando um dos métodos anteriores.

Esse padrão só está disponível Regiões da AWS onde AWS Control Tower está disponível, inclusive AWS GovCloud (US).

Ativando e desativando controles no padrão

Depois de criar o padrão no AWS Control Tower console, você pode ver o padrão e seus controles disponíveis nos dois serviços.

Depois de criar o padrão pela primeira vez, ele não tem nenhum controle ativado automaticamente. Além disso, quando o Security Hub adiciona novos controles, eles não são habilitados automaticamente para o Service-Managed Standard:. AWS Control Tower Você deve ativar e desativar os controles para o padrão in AWS Control Tower usando um dos seguintes métodos:

- AWS Control Tower console
- AWS Control Tower API (chame as `DisableControl`APIs `EnableControl`e)
- AWS CLI (execute os `disable-control`comandos `enable-control`e)

Quando você altera o status de habilitação de um controle em AWS Control Tower, a alteração também é refletida no Security Hub.

No entanto, desabilitar um controle no Security Hub que está ativado AWS Control Tower resulta em desvio de controle. O status do controle em é AWS Control Tower exibido como`Drifted`. Você pode

resolver esse desvio selecionando Registrar novamente a OU no AWS Control Tower console ou desativando e reativando o controle AWS Control Tower usando um dos métodos anteriores.

A conclusão das ações de ativação e desativação AWS Control Tower ajuda a evitar desvios de controle.

Quando você ativa ou desativa os controles em AWS Control Tower, a ação se aplica a todas as contas e regiões. Se você ativar e desativar os controles no Security Hub (não recomendado para esse padrão), a ação se aplicará somente à conta atual e à região.

> **Note**
>
> A configuração central não pode ser usada para gerenciar o Service-Managed Standard:. AWS Control Tower Se você usar a configuração central, poderá usar somente o AWS Control Tower serviço para ativar e desativar os controles desse padrão para uma conta gerenciada centralmente.

Visualizando o status da habilitação e o status do controle

É possível exibir o status de habilitação de um controle usando um dos métodos a seguir:

- Console do Security Hub, API do Security Hub ou AWS CLI
- AWS Control Tower console
- AWS Control Tower API para ver uma lista de controles habilitados (chame a `ListEnabledControls`API)
- AWS CLI para ver uma lista de controles habilitados (execute o `list-enabled-controls`comando)

Um controle que você desabilita AWS Control Tower tem um status de habilitação `Disabled` no Security Hub, a menos que você habilite explicitamente esse controle no Security Hub.

O Security Hub calcula o status do controle com base no status do fluxo de trabalho e no status de conformidade das descobertas de controle. Para obter mais informações sobre o status de habilitação e o status de controle, consulte Visualizar detalhes de controles.

Com base nos status de controle, o Security Hub calcula uma pontuação de segurança para o Service-Managed Standard:. AWS Control Tower Essa pontuação só está disponível no Security

Hub. Além disso, você só pode visualizar as descobertas de controle no Security Hub. A pontuação de segurança padrão e as descobertas de controle não estão disponíveis em AWS Control Tower.

> **Note**
>
> Quando você ativa controles para Service-Managed Standard: AWS Control Tower, o Security Hub pode levar até 18 horas para gerar descobertas para controles que usam uma regra vinculada ao AWS Config serviço existente. É possível ter regras vinculadas a serviços existentes se tiver habilitado outros padrões e controles no Security Hub. Para ter mais informações, consulte Programar a execução de verificações de segurança.

Excluindo o padrão

Você pode excluir esse padrão AWS Control Tower desativando todos os controles aplicáveis usando um dos seguintes métodos:

- AWS Control Tower console
- AWS Control Tower API (chame a `DisableControl`API)
- AWS CLI (execute o `disable-control`comando)

A desativação de todos os controles exclui o padrão em todas as contas gerenciadas e regiões governadas no AWS Control Tower. A exclusão do padrão em o AWS Control Tower remove da página Padrões do console do Security Hub, e você não pode mais acessá-lo usando a API do Security Hub ou AWS CLI.

> **Note**
>
> Desabilitar todos os controles do padrão no Security Hub não desativa nem exclui o padrão.

A desativação do serviço Security Hub remove o Service-Managed Standard: AWS Control Tower e quaisquer outros padrões que você tenha habilitado.

Localizando o formato de campo para o Service-Managed Standard: AWS Control Tower

Ao criar o Service-Managed Standard: AWS Control Tower e habilitar controles para ele, você começará a receber descobertas de controle no Security Hub. O Security Hub relata as descobertas

de controle no AWS Formato de descoberta de segurança (ASFF). Esses são os valores ASFF para o nome do recurso da Amazon (ARN) desse padrão e `GeneratorId`:

- ARN padrão — *`arn:aws:us-east-1`*`:securityhub:::standards/service-managed-aws-control-tower/v/1.0.0`
- GeneratorId – `service-managed-aws-control-tower/v/1.0.0/`*`CodeBuild.1`*

Para obter um exemplo de descoberta do Service-Managed Standard: AWS Control Tower, consulte. Exemplo de descobertas de controle

Controles que se aplicam ao padrão gerenciado por serviços: AWS Control Tower

Padrão gerenciado por serviços: AWS Control Tower suporta um subconjunto de controles que fazem parte do padrão AWS Foundational Security Best Practices (FSBP). Escolha um controle na tabela a seguir para ver informações sobre ele, incluindo etapas de correção para descobertas malsucedidas.

A lista a seguir mostra os controles disponíveis para o Service-Managed Standard:. AWS Control Tower Os limites regionais dos controles correspondem aos limites regionais dos controles corolários no padrão FSBP. Essa lista mostra IDs de controle de segurança independentes do padrão. No AWS Control Tower console, os IDs de controle são formatados como SH. ***`ControlID (`***por exemplo, SH). CodeBuild.1). No Security Hub, se as descobertas de controle consolidadas estiverem desativadas em sua conta, o campo `ProductFields.ControlId` usará o ID de controle baseado em padrão. O ID de controle baseado em padrões é formatado como CT. ***`ControlId`***(por exemplo, CT. CodeBuild.1).

- [Conta.1] As informações de contato de segurança devem ser fornecidas para um Conta da AWS
- Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- [ApiGateway.1] O REST do API Gateway WebSocket e o registro de execução da API devem estar habilitados
- Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end
- Os estágios da API REST de Gateway devem ter o rastreamento AWS X-Ray habilitado.
- O API Gateway deve ser associado a uma WAF Web ACL

- Os dados do cache da API REST de Gateway devem ser criptografados em repouso
- As rotas do API de Gateway devem especificar um tipo de autorização
- O registro de acesso deve ser configurado para os estágios V2 do API de Gateway
- [AppSync.5] As APIs AWS AppSync do GraphQL não devem ser autenticadas com chaves de API
- [AutoScaling.1] Grupos de Auto Scaling associados a um balanceador de carga devem usar verificações de integridade do ELB
- [AutoScaling.2] O grupo Amazon EC2 Auto Scaling deve abranger várias zonas de disponibilidade
- [AutoScaling.3] As configurações de lançamento de grupos do Auto Scaling devem configurar as instâncias do EC2 para exigir o Instance Metadata Service Version 2 (IMDSv2)
- As instâncias do Amazon EC2 lançadas usando as configurações de execução em grupo do Auto Scaling não devem ter endereços IP públicos
- [AutoScaling.6] Os grupos de Auto Scaling devem usar vários tipos de instância em várias zonas de disponibilidade
- [AutoScaling.9] Os grupos do Amazon EC2 Auto Scaling devem usar os modelos de lançamento do Amazon EC2
- [CloudTrail.1] CloudTrail deve ser habilitado e configurado com pelo menos uma trilha multirregional que inclua eventos de gerenciamento de leitura e gravação
- [CloudTrail.2] CloudTrail deve ter a criptografia em repouso ativada
- [CloudTrail.4] a validação do arquivo de CloudTrail log deve estar ativada
- [CloudTrail.5] CloudTrail trilhas devem ser integradas com o Amazon CloudWatch Logs
- [CloudTrail.6] Certifique-se de que o bucket do S3 usado para armazenar CloudTrail registros não esteja acessível ao público
- [CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais
- [CodeBuild.2] as variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado
- [CodeBuild.3] Os registros do CodeBuild S3 devem ser criptografados
- [CodeBuild.4] ambientes de CodeBuild projeto devem ter uma duração de registro AWS Config
- As instâncias de replicação do PCI.DMS.1 Database Migration Service não devem ser públicas
- Os endpoints do DMS devem usar SSL
- Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado

- Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos
- As tabelas do DynamoDB devem escalar automaticamente a capacidade de acordo com a demanda
- [DynamoDB.2] As tabelas do DynamoDB devem ter a recuperação ativada point-in-time
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [PCI.EC2.1] Os instantâneos do Amazon EBS não devem ser restauráveis publicamente
- [EC2.2] O grupo de segurança padrão da VPC não deve permitir o tráfego de entrada e saída
- [EC2.3] Os volumes anexados do Amazon EBS devem ser criptografados em repouso.
- As instâncias EC2 interrompidas devem ser removidas após um período de tempo especificado
- [EC2.6] O registro de fluxo de VPC deve ser ativado em todas as VPCs
- [EC2.7] A criptografia padrão do EBS deve estar ativada
- As instâncias do EC2 devem usar o Instance Metadata Service Version 2 (IMDSv2)
- As instâncias do Amazon EC2 não devem ter um endereço IPv4 público
- O Amazon EC2 deve ser configurado para usar endpoints da VPC criados para o serviço Amazon EC2
- As sub-redes do Amazon EC2 não devem atribuir automaticamente endereços IP públicos
- As listas de controle de acesso à rede não utilizadas devem ser removidas
- As instâncias do Amazon EC2 não devem usar vários ENIs
- Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas
- Grupos de segurança não devem permitir acesso irrestrito a portas com alto risco
- [EC2.20] Ambos os túneis VPN para uma conexão VPN Site-to-Site devem estar ativos AWS
- As ACLs de rede não devem permitir a entrada de 0.0.0.0/0 para a porta 22 ou porta 3389
- [PCI.EC2.3] Os grupos de segurança do Amazon EC2 devem ser removidos
- Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC
- Os modelos de lançamento do Amazon EC2 não devem atribuir IPs públicos às interfaces de rede
- Os repositórios privados do ECR devem ter a digitalização de imagens configurada
- [ECR.2] Os repositórios privados do ECR devem ter a imutabilidade da tag configurada
- Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada
- As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário.

- Os serviços do ECS não devem ter endereços IP públicos atribuídos a eles automaticamente
- As definições de tarefas do ECS não devem compartilhar o namespace do processo do host
- Os contêineres ECS devem ser executados sem privilégios
- Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz
- Os segredos não devem ser passados como variáveis de ambiente do contêiner
- Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate
- Os clusters do ECS devem usar Container Insights
- [EFS.1] O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS
- [EFS.2] Os volumes do Amazon EFS devem estar em planos de backup
- Os pontos de acesso do EFS devem impor um diretório raiz
- Os pontos de acesso do EFS devem impor uma identidade de usuário
- Os endpoints do cluster EKS não devem ser acessíveis ao público
- Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [ElastiCache.3] ElastiCache para grupos de replicação do Redis, o failover automático deve estar ativado
- [ElastiCache.4] ElastiCache para Redis, os grupos de replicação devem ser criptografados em repouso
- [ElastiCache.5] ElastiCache para Redis, os grupos de replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache para grupos de replicação do Redis antes da versão 6.0 deve usar o Redis AUTH
- [ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de integridade aprimorados habilitados
- [ElasticBeanstalk.2] As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas
- [ELBv2.1] O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS
- [ELB.2] Os balanceadores de carga clássicos com ouvintes SSL/HTTPS devem usar um certificado fornecido pelo AWS Certificate Manager

- Os receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS
- O Application Load Balancer deve ser configurado para eliminar cabeçalhos http
- O registro em log do Classic Load Balancer e Application Load Balancer deve estar ativado
- [ELB.6] Os balanceadores de carga de aplicativos, gateways e redes devem ter a proteção contra exclusão ativada
- Os Classic Load Balancers devem ter a drenagem da conexão ativada
- [ELB.8] Os balanceadores de carga clássicos com ouvintes SSL devem usar uma política de segurança predefinida que tenha uma duração forte AWS Config
- Os Classic Load Balancers devem ter o balanceador de carga entre zonas habilitado
- Verifica se o Classic Load Balancer abrange várias zonas de disponibilidade (AZs).
- O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- Balanceadores de carga de aplicações, redes e gateways não abrangem várias zonas de disponibilidade
- O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [EMR.1] Os nós primários do cluster do Amazon EMR não devem ter endereços IP públicos
- [ES.1] Os domínios do devem ter a criptografia em repouso habilitada.
- [ES.2] Os domínios do Elasticsearch não devem ser publicamente acessíveis
- Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós
- [ES.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado
- Os domínios do Elasticsearch devem ter o registro em log de auditoria ativado
- Os domínios do Elasticsearch devem ter pelo menos três nós de dados
- Os domínios do Elasticsearch devem ser configurados com pelo menos três nós principais dedicados
- [ES.8] As conexões com os domínios do Elasticsearch devem ser criptografadas usando a política de segurança TLS mais recente
- [EventBridge.3] os ônibus de eventos EventBridge personalizados devem ter uma política baseada em recursos anexada
- [GuardDuty.1] GuardDuty deve ser ativado
- [IAM.1] As políticas do não devem permitir privilégios administrativos completos "*"

- [IAM.2] Os usuários do não devem ter políticas do IAM anexadas
- [IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos
- [IAM.4] A chave de acesso do usuário raiz do não deve existir
- [IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- [IAM.7] As políticas de senha para usuários do IAM devem ter configurações fortes
- As credenciais de usuário do IAM não utilizadas devem ser removidas
- As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- Os fluxos do Kinesis devem ser criptografados em repouso
- As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS
- [KMS.3] não AWS KMS keys deve ser excluído acidentalmente
- A rotação de AWS KMS teclas [KMS.4] deve estar ativada
- [PCI.lambda.1] As funções do devem proibir o acesso público
- [Lambda.2] As funções do devem usar os tempos de execução mais recentes
- [PCI.Lambda.2] As funções do Lambda devem estar em uma VPC
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- Os clusters de banco de dados Neptune devem ter backups automatizados habilitados
- Os clusters de banco de dados Neptune devem ser criptografados em repouso

- [Neptune.7] Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- [NetworkFirewall.3] As políticas de Firewall de Rede devem ter pelo menos um grupo de regras associado
- [NetworkFirewall.4] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar pacotes completos
- [NetworkFirewall.5] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar para pacotes fragmentados
- [NetworkFirewall.6] O grupo de regras do Stateless Network Firewall não deve estar vazio
- Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada
- Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público
- Os OpenSearch domínios [Opensearch.3] devem criptografar os dados enviados entre os nós
- O registro de erros de OpenSearch domínio [Opensearch.4] nos CloudWatch registros deve estar ativado
- Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado
- Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados
- Os OpenSearch domínios [Opensearch.7] devem ter um controle de acesso refinado ativado
- [Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente
- [RDS.1] Os instantâneos do RDS devem ser privados
- [RDS.2] As instâncias de banco de dados do RDS devem proibir o acesso público, conforme determinado pela duração PubliclyAccessible AWS Config
- [RDS.3] As instâncias de banco de dados do RDS devem ter a criptografia em repouso habilitada.
- Os instantâneos do cluster do RDS e os instantâneos do banco de dados devem ser criptografados em repouso
- As instâncias de banco de dados do RDS devem ser configuradas com várias zonas de disponibilidade
- O monitoramento aprimorado deve ser configurado para instâncias de banco de dados do RDS
- [RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada
- [RDS.9] As instâncias de banco de dados do RDS devem publicar registros no Logs CloudWatch

- A autenticação do IAM deve ser configurada para instâncias do RDS
- As instâncias do RDS devem ter backups automáticos habilitados
- A autenticação do IAM deve ser configurada para instâncias do RDS
- [RDS.13] As atualizações automáticas de versões secundárias do RDS devem ser ativadas
- [RDS.15] Os clusters de banco de dados do RDS devem ser configurados para várias zonas de disponibilidade
- As instâncias de banco de dados do RDS devem ser configuradas para copiar tags para instantâneos
- As instâncias do RDS devem ser implantadas em uma VPC
- As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de cluster
- As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de cluster
- Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de parâmetros do banco de dados
- Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de parâmetros do banco de dados
- As instâncias do RDS não devem usar uma porta padrão do mecanismo de banco de dados
- Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [PCI.Redshift.1] Os clusters do devem proibir o acesso público
- As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito
- Os clusters do Amazon Redshift devem ter o registro de auditoria ativado
- O Amazon Redshift deve ter as atualizações automáticas para as versões principais habilitadas
- Os clusters do Redshift devem usar roteamento de VPC aprimorado
- Os clusters do Amazon Redshift não devem usar o nome de usuário Admin padrão
- [Redshift.9] Os clusters do Redshift não devem usar o nome do banco de dados padrão
- [Redshift.10] Os clusters do Redshift devem ser criptografados em repouso
- [S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas

- [S3.2] Os buckets de uso geral do S3 devem bloquear o acesso público de leitura
- [S3.3] Os buckets de uso geral do S3 devem bloquear o acesso público de gravação
- [S3.5] Os buckets de uso geral do S3 devem exigir solicitações de uso de SSL
- [S3.6] As políticas de bucket de uso geral do S3 devem restringir o acesso a outros Contas da AWS
- [S3.8] Os buckets de uso geral do S3 devem bloquear o acesso público
- [S3.9] Os buckets de uso geral do S3 devem ter o registro de acesso ao servidor ativado
- [S3.12] As ACLs não devem ser usadas para gerenciar o acesso do usuário aos buckets de uso geral do S3
- [S3.13] Os buckets de uso geral do S3 devem ter configurações de ciclo de vida
- [S3.17] Os buckets de uso geral do S3 devem ser criptografados em repouso com AWS KMS keys
- [SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet
- [SageMaker.2] as instâncias do SageMaker notebook devem ser iniciadas em uma VPC personalizada
- [SageMaker.3] Os usuários não devem ter acesso root às instâncias do SageMaker notebook
- [SecretsManager.1] Os segredos do Secrets Manager devem ter a rotação automática ativada
- [SecretsManager.2] Os segredos do Secrets Manager configurados com rotação automática devem girar com sucesso
- [SecretsManager.3] Remover segredos não utilizados do Secrets Manager
- [SecretsManager.4] Os segredos do Secrets Manager devem ser alternados dentro de um determinado número de dias
- As filas do Amazon SQS devem ser criptografadas em repouso
- [SSM.1] As instâncias do Amazon EC2 devem ser gerenciadas por AWS Systems Manager
- [PCI.SSM.1] As instâncias do Amazon EC2 gerenciadas pelo devem ter um status de conformidade de patch de COMPLIANT (Em conformidade) após a instalação do patch
- PCI.SSM.2 As instâncias de Amazon EC2 gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- Os documentos SSM não devem ser públicos
- [WAF.2] As regras regionais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.3] Os grupos de regras regionais AWS WAF clássicos devem ter pelo menos uma regra

- [WAF.4] As ACLs regionais AWS WAF clássicas da web devem ter pelo menos uma regra ou grupo de regras
- [WAF.10] as ACLs AWS WAF da web devem ter pelo menos uma regra ou grupo de regras

Para obter mais informações sobre o Security Hub, consulte o Guia do usuário do .

Visualizando e gerenciando padrões de segurança

Os padrões de segurança incluem um conjunto de requisitos para determinar a conformidade com estruturas regulatórias, melhores práticas do setor ou políticas da empresa. AWS Security Hub mapeia esses requisitos para controles e executa verificações de segurança nos controles para avaliar se os requisitos de um padrão estão sendo atendidos. Um controle pode ser ativado em um ou mais padrões. Se você ativar as descobertas de controle consolidadas, o Security Hub gerará uma única descoberta para uma verificação de segurança, mesmo quando o controle estiver incluído em vários padrões habilitados. Para ter mais informações, consulte Ativar/desativar descobertas de controle consolidadas.

Para obter uma lista dos padrões disponíveis e os controles que se aplicam a eles, consulte Referência de padrões. A página Padrões de segurança no console do Security Hub também mostra todos os padrões de segurança suportados no Security Hub e seu status de ativação. Para cada padrão de segurança ativado em sua conta (ou se você usa a integração com AWS Organizations, em pelo menos uma conta em sua organização), você pode visualizar as seguintes informações:

- O status de habilitação do padrão em diferentes políticas de configuração do Security Hub se você usar a configuração central
- Uma descrição de quaisquer padrões desabilitados
- Uma lista dos controles atualmente habilitados no padrão e o status geral desses controles com base no status de conformidade de suas descobertas
- uma lista de controles que se aplicam ao padrão, mas estão atualmente desabilitados.
- Uma pontuação de segurança para o padrão

O Security Hub gera uma pontuação de segurança para cada padrão. As contas de administrador veem pontuações de segurança agregadas e status de controle em suas contas-membro. Se você definiu uma região de agregação, suas pontuações de segurança refletem o status de conformidade dos controles em todas as regiões vinculadas. Para ter mais informações, consulte Como as pontuações de segurança são calculadas.

Tópicos

Disabling or enabling a security standard (Desabilitar ou habilitar um padrão de segurança)

É possível ativar ou desativar cada padrão de segurança disponível no Security Hub.

Antes de ativar qualquer padrão de segurança, verifique se você ativou AWS Config e configurou a gravação de recursos. Caso contrário, o Security Hub talvez não consiga gerar descobertas para os controles que se aplicam a um padrão. Para ter mais informações, consulte Configurando AWS Config.

> **Note**
>
> As instruções para habilitar e desabilitar os padrões variam de acordo com o uso ou não da configuração central. Esta seção descreve as diferenças. A configuração central está disponível para usuários que integram o Security Hub AWS Organizations e. Recomendamos usar a configuração central para simplificar o processo de habilitação e desabilitação de padrões em ambientes com várias contas e várias regiões.

Habilitar um padrão de segurança (API)

Ao habilitar um padrão de segurança, todos os controles para esse padrão são habilitados por padrão. O Security Hub também começa a gerar descobertas para controles que se aplicam ao padrão.

É possível escolher quais controles habilitar e desabilitar em cada padrão. A desativação de um controle impede que as descobertas do controle sejam geradas, e o controle é ignorado ao calcular as pontuações de segurança.

Quando você habilita o Security Hub pela primeira vez, o Security Hub calcula a pontuação de segurança resumida e as pontuações de segurança padrão dentro de 30 minutos após sua primeira visita à página Resumo ou à página Padrões de Segurança no console do Security Hub. Pode levar

até 24 horas para que as pontuações de segurança pela primeira vez sejam geradas nas regiões da China e AWS GovCloud (US) Region. As pontuações são geradas somente para padrões que são ativados quando você visita essas páginas. Além disso, o registro AWS Config de recursos deve ser configurado para que as pontuações apareçam. Após a primeira geração de pontuação, o Security Hub atualiza as pontuações de segurança a cada 24 horas. O Security Hub exibe um timestamp para indicar quando uma pontuação de segurança foi atualizada pela última vez. Para ver uma lista dos padrões atualmente habilitados na sua conta, invoque a API GetEnabledStandards.

Habilitação de um padrão em várias contas e regiões

Para habilitar um padrão de segurança em várias contas Regiões da AWS, você deve usar a configuração central.

Quando você usa a configuração central, o administrador delegado pode criar políticas de configuração do Security Hub que habilitem um ou mais padrões. Em seguida, é possível associar a política de configuração a contas e unidades organizacionais (OUs) específicas ou à raiz. Uma política de configuração entra em vigor na sua região inicial (também chamada de região de agregação) e em todas as regiões vinculadas.

As políticas de configuração oferecem personalização. Por exemplo, você pode optar por habilitar somente as Melhores Práticas de AWS Segurança Fundamental (FSBP) em uma OU, e você pode optar por habilitar o FSBP e o Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 em outra OU. Para obter instruções sobre como criar uma política de configuração que habilite padrões específicos, consulte Criação e associação de políticas de configuração do Security Hub

Se você usa a configuração central, o Security Hub não habilita automaticamente nenhum padrão em contas novas ou existentes. Em vez disso, ao criar uma política de configuração, o administrador delegado define quais padrões devem ser habilitados em diferentes contas. O Security Hub oferece uma política de configuração recomendada na qual somente o FSBP está habilitado. Para ter mais informações, consulte Tipos de políticas de configuração.

> **Note**
>
> O administrador delegado pode criar políticas de configuração para habilitar qualquer padrão, exceto o Padrão Gerenciado por Serviços:. AWS Control Tower Você pode ativar esse padrão somente no AWS Control Tower serviço. Se você usar a configuração central, poderá usar habilitar e desabilitar controles nesse padrão para uma conta gerenciada centralmente somente no AWS Control Tower.

Se você quiser que algumas contas configurem seus próprios padrões em vez do administrador delegado, o administrador delegado pode designar essas contas como autogerenciadas. As contas autogerenciadas devem configurar padrões separadamente em cada região.

Habilitação de um padrão em uma única conta e região

Se você não usar a configuração central ou se você for uma conta autogerenciada, não poderá usar políticas de configuração para habilitar padrões de forma centralizada em várias contas e regiões. Contudo, é possível usar as etapas a seguir para habilitar um padrão em uma única conta e região.

Security Hub console

Para habilitar um padrão em uma conta e região

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. Verifique se você está usando o na região na qual deseja desabilitar o padrão.
3. No painel de navegação do Security Hub, selecione Padrões de segurança.
4. Para o padrão que deseja habilitar, selecione Enable (Habilitar). Isso também habilita todos os controles dentro desse padrão.
5. Repita em cada região na qual deseja habilitar o padrão.

Security Hub API

Para habilitar um padrão em uma conta e região

1. Invoque a API BatchEnableStandards.
2. Forneça o Nome do recurso da Amazon (ARN) do padrão que deseja habilitar. Para obter o ARN padrão, invoque a API DescribeStandards.
3. Repita em cada região na qual deseja habilitar o padrão.

AWS CLI

Para habilitar um padrão em uma conta e região

1. Execute o comando batch-enable-standards.
2. Forneça o Nome do recurso da Amazon (ARN) do padrão que deseja habilitar. Para obter o ARN padrão, execute o comando describe-standards.

```
aws securityhub batch-enable-standards --standards-subscription-requests
 '{"StandardsArn": "standard ARN"}'
```

Exemplo

```
aws securityhub batch-enable-standards --standards-subscription-requests
 '{"StandardsArn":"arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"}'
```

3. Repita em cada região na qual deseja habilitar o padrão.

Habilitação automática de padrões de segurança padrão

Se você não usa a configuração central, o Security Hub habilita automaticamente os padrões de segurança padrão em novas contas quando elas ingressam na sua organização. Todos os controles que fazem parte dos padrões padrão também são habilitados automaticamente. Atualmente, os padrões de segurança padrão que são habilitados automaticamente são AWS Foundational Security Best Practices (FSBP) e Center for Internet Security (CIS) Foundations Benchmark v1.2.0. AWS É possível desativar os padrões habilitados automaticamente se preferir habilitá-los manualmente em novas contas.

Se você usar a configuração central, poderá criar uma política de configuração que habilite os padrões padrão e associar essa política à raiz. Todas as contas e OUs da sua organização herdarão essa política de configuração, a menos que estejam associadas a uma política diferente ou sejam autogerenciadas.

Desativação de padrões habilitados automaticamente

As etapas a seguir se aplicam somente se você integra com a configuração central, AWS Organizations mas não usa. Se você não usar a integração Organizations, poderá desativar um padrão ao habilitar o Security Hub pela primeira vez ou seguir as etapas para desabilitar um padrão.

Security Hub console

Para desativar padrões habilitados automaticamente

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

   Faça login no console do usando as credenciais de um administrador da .

2. No painel de navegação do Security Hub, em Configurações, escolha Configuração.
3. Na seção Contas, desative os Habilitar automaticamente padrões padrão.

Security Hub API

Para desativar padrões habilitados automaticamente

1. Invoque a API UpdateOrganizationConfiguration na conta do administrador do Security Hub.
2. Para desativar os padrões habilitador automaticamente em novas contas-membro, defina `AutoEnableStandards` igual a `NONE`.

AWS CLI

Para desativar padrões habilitados automaticamente

1. Execute o comando update-organization-configuration.
2. Inclua o parâmetro `auto-enable-standards` para desativar os padrões habilitados automaticamente em novas contas-membro.

```
aws securityhub update-organization-configuration --auto-enable-standards
```

Desabilitar um padrão de segurança (API)

Ao desabilitar um padrão de segurança no Security Hub, ocorre o seguinte:

- Todos os controles que se aplicam ao padrão também são desativados, a menos que estejam associados a outro padrão.
- Quando você desabilitar um controle, a verificação do controle não será mais realizada e nenhuma descoberta adicional será gerada.
- As descobertas existentes para controles desabilitados são arquivadas automaticamente após aproximadamente 3 a 5 dias.
- As AWS Config regras que o Security Hub criou para os controles desativados foram removidas.

  Isso normalmente ocorre alguns minutos após a desativação do padrão, mas pode levar mais tempo. Se a primeira solicitação para excluir AWS Config as regras falhar, o Security Hub tentará novamente a cada 12 horas. Entretanto, se você desabilitou o Security Hub ou não tem nenhum

outro padrão habilitado, o Security Hub não poderá repetir a solicitação, o que significa que ele não poderá excluir as regras da AWS Config . Se isso ocorrer e você precisar excluir AWS Config regras, entre em contato AWS Support.

Desabilitação de um padrão em várias contas e regiões

Para desabilitar um padrão de segurança em várias contas e regiões, você deve usar a configuração central.

Quando você usa a configuração central, o administrador delegado pode criar políticas de configuração que desabilitem um ou mais padrões. É possível associar a política de configuração a contas e unidades organizacionais (OUs) específicas ou à raiz. Uma política de configuração entra em vigor na sua região inicial (também chamada de região de agregação) e em todas as regiões vinculadas.

As políticas de configuração oferecem personalização. Por exemplo, é possível optar por desabilitar o Payment Card Industry Data Industry Data Security Data Security (PCI DSS) em uma OU e pode optar por desabilitar o PCI DSS e o National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 em outra OU. Para obter instruções sobre como criar uma política de configuração que desabilite padrões específicos, consulte Criação e associação de políticas de configuração do Security Hub.

> **Note**
>
> O administrador delegado pode criar políticas de configuração para desativar qualquer padrão, exceto o Padrão Gerenciado por Serviços:. AWS Control Tower Você pode desativar esse padrão somente no AWS Control Tower serviço. Se você usar a configuração central, poderá usar habilitar e desabilitar controles nesse padrão para uma conta gerenciada centralmente somente no AWS Control Tower.

Se você quiser que algumas contas configurem seus próprios padrões em vez do administrador delegado, o administrador delegado pode designar essas contas como autogerenciadas. As contas autogerenciadas devem configurar padrões separadamente em cada região.

Desabilitação de um padrão em uma única conta e região

Se você não usar a configuração central ou se você for uma conta autogerenciada, não poderá usar políticas de configuração para desabilitar padrões de forma centralizada em várias contas e

regiões. Contudo, é possível usar as etapas a seguir para desabilitar um padrão em uma única conta e região.

Security Hub console

Para desabilitar um padrão em uma conta e região

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. Verifique se você está usando o na região na qual deseja desabilitar o padrão.
3. No painel de navegação do Security Hub, selecione Padrões de segurança.
4. Para o padrão que deseja desativar, selecione Disable (Desabilitar).
5. Repita em cada região na qual deseja desabilitar o padrão.

Security Hub API

Para desabilitar um padrão em uma conta e região

1. Invoque a API BatchDisableStandards.
2. Para cada padrão que você deseja desativar, forneça o ARN da assinatura padrão. Para obter os ARNs de assinatura para seus padrões habilitados, invoque a API GetEnabledStandards.
3. Repita em cada região na qual deseja desabilitar o padrão.

AWS CLI

Para desabilitar um padrão em uma conta e região

1. Execute o comando batch-disable-standards.
2. Para cada padrão que você deseja desativar, forneça o ARN da assinatura padrão. Para obter os ARNs de assinatura para seus padrões habilitados, execute o comando get-enabled-standards.

```
aws securityhub batch-disable-standards --standards-subscription-arns "standard
 subscription ARN"
```

Exemplo

```
aws securityhub batch-disable-standards --standards-subscription-arns
 "arn:aws:securityhub:us-west-1:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0"
```

3. Repita em cada região na qual deseja desabilitar o padrão.

Visualizando detalhes de um padrão

No AWS Security Hub console, a página de detalhes de um padrão inclui as seguintes informações:

- A pontuação de segurança padrão e um resumo visual das verificações de segurança dos controles habilitados no padrão. Se você se integrar com AWS Organizations, os controles habilitados em pelo menos uma conta da organização serão considerados ativados.
- As configurações para habilitar ou desabilitar um controle que se aplica ao padrão.
- Controles que se aplicam ao padrão FSBP Os controles são divididos em guias diferentes com base no status de ativação. O número de controles na coluna Todos habilitados é a soma dos controles nas colunas Falha, Desconhecido, Sem dados e Aprovado.

Você também pode usar a API do Security Hub e AWS CLI recuperar detalhes de um padrão. As seções a seguir explicam como obter detalhes de um padrão.

Visualizar os controles de um padrão habilitado

Na página Padrões de segurança, é possível exibir a página de detalhes de um padrão ativado.

Se você estiver conectado à conta de administrador, poderá ver os detalhes de qualquer padrão habilitado em pelo menos uma conta-membro.

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação do Security Hub, selecione Padrões de segurança.
3. Para o padrão para o qual deseja desabilitar os controles, escolha View results (Visualizar resultados).

Pontuação de segurança padrão e resumo das verificações de segurança

Na parte superior da página de detalhes padrão está a pontuação de segurança do padrão. A pontuação é a porcentagem de controles aprovados em relação ao número de controles habilitados (que têm dados) para o padrão.

Normalmente, o Security Hub gera o status inicial do controle dentro de 30 minutos após sua primeira visita à página Resumo ou à página Padrões de segurança no console do Security Hub. As pontuações são geradas somente para padrões que são ativados quando você visita essas páginas. Para ver uma lista dos padrões atualmente habilitados, invoque a operação da API `GetEnabledStandards`. Além disso, a gravação de recursos AWS Config deve ser configurada para que o status do controle apareça. Após a primeira geração de pontuação, o Security Hub atualiza as pontuações de segurança a cada 24 horas. O Security Hub exibe um timestamp para indicar quando uma pontuação de segurança foi atualizada pela última vez. Para ter mais informações, consulte the section called “Determinando as pontuações de segurança”.

> **Note**
>
> Pode levar até 24 horas para que as pontuações de segurança pela primeira vez sejam geradas nas regiões da China e AWS GovCloud (US) Region.

Ao lado da pontuação, há um gráfico que resume as verificações de segurança dos controles habilitados para o padrão. O gráfico mostra a porcentagem de verificações de segurança reprovadas e aprovadas. Quando você faz uma pausa no gráfico, o pop-up exibe o seguinte:

- O número de verificações de segurança que falharam nos controles de cada severidade
- O número de verificações de segurança para controles com status Desconhecido
- O número de verificações de segurança aprovadas

Para contas de administrador, o status de controle reflete o status agregado da conta do administrador e de todas as contas dos membros.

Todos os dados nas páginas de detalhes dos Padrões de segurança são específicos da região atual, a menos que você tenha definido uma região de agregação. Se você definiu uma região de agregação, as pontuações de segurança se aplicam a todas as regiões e incluem descobertas em todas as regiões vinculadas. O status de conformidade dos controles nas páginas de detalhes dos

padrões também reflete as descobertas das regiões vinculadas, e o número de verificações de segurança inclui as descobertas das regiões vinculadas.

Visualizando os controles em padrões habilitados

Ao visitar a página de detalhes de um padrão, é possível ver uma lista dos controles de segurança que se aplicam ao padrão. Essa lista é classificada com base no status de conformidade do controle e na severidade atribuída a cada controle. O Security Hub atualiza os status de controle e a contagem de verificações de segurança a cada 24 horas. Um timestamp em cada guia indica quando os status de controle e a contagem de verificações de segurança foram atualizados mais recentemente. Para ter mais informações, consulte the section called “Status de conformidade e status de controle”.

Para contas de administrador, o status de controle reflete o status agregado da conta do administrador e de todas as contas dos membros.

A guia Todos habilitados lista todos os controles atualmente habilitados no padrão. Para contas de administrador, a guia Todos habilitados inclui controles que estão habilitados no padrão em suas contas ou em pelo menos uma conta-membro.

Nas guias Falha, Desconhecido, Sem dados e Aprovado, os controles da guia Todos ativados são filtrados para incluir somente controles habilitados com um status específico.

A guia Desativado contém a lista de controles que estão desativados no padrão. Para contas de administrador, a guia Todos habilitados inclui controles que estão habilitados no padrão em suas contas ou em pelo menos uma conta-membro.

Para cada controle, as guias exibem as seguintes informações:

- O status geral do controle
- A severidade associada ao controle
- Título e ID do controle
- O número de descobertas ativas que falharam em relação ao número total de descobertas ativas. Se aplicável, a coluna Verificações falhadas também lista o número de descobertas com o status Desconhecido.

Além do filtro de pesquisa em cada guia, é possível classificar as listas com base nos seguintes campos:

- Compliance status (Status de conformidade)
- Gravidade
- ID
- Título
- Verificações com falha

É possível classificar cada lista usando qualquer uma das colunas. Por padrão, a guia Todos ativados é classificada de forma que os controles com falha estejam no topo da lista. Isso ajuda você a se concentrar imediatamente nos problemas que precisam ser corrigidos.

Nas guias restantes, os controles são classificados por padrão em ordem decrescente por severidade. Em outras palavras, os controles críticos são primeiro, seguidos pelos controles de severidade alta, depois média e depois baixa.

Escolha seu método de acesso preferido e siga as etapas para exibir os controles disponíveis para um padrão ativado. Em vez dessas instruções, você também pode usar a operação da DescribeStandardsControlAPI.

Security Hub console

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação do , selecione Security standards (Padrões de segurança).
3. Escolha Exibir resultados para um padrão. A parte inferior da página lista os controles (divididos por guias) que se aplicam ao padrão.

Security Hub API

1. Execute `ListSecurityControlDefinitions` e forneça um nome do recurso da Amazon (ARN) padrão para obter uma lista de IDs de controle para esse padrão. Para obter o ARN padrão, execute `DescribeStandards`. Se você não fornecer um ARN padrão, essa API retornará todas as IDs de controle do Security Hub. Essa API retorna IDs de controle de segurança independentes do padrão, não IDs de controle específicos do padrão.

   Exemplo de solicitação

   ```
   {
   ```

```
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
best-practices/v/1.0.0"
}
```

2. Execute ListStandardsControlAssociations para descobrir se um controle está ativado em cada padrão que você ativou em sua conta.
3. Identifique o controle fornecendo `SecurityControlId` ou `SecurityControlArn`. Os parâmetros de paginação são opcionais.

   Exemplo de solicitação

```
{
    SecurityControlId: Config.1
    NextToken: lkeyusdlk-sdlflsnd-ladfterb
    MaxResults: 5
}
```

AWS CLI

1. Execute o comando `list-security-control-definitions` e forneça um ou mais ARNs padrão para obter uma lista de IDs de controle. Para obter o ARN padrão, execute `describe-standards`. Se você não fornecer um ARN padrão, essa API retornará todas as IDs de controle do Security Hub. Essa API retorna IDs de controle de segurança independentes do padrão, não IDs de controle específicos do padrão.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Execute `list-standards-control-associations` para descobrir se um controle está ativado em cada padrão que você ativou em sua conta.
3. Identifique o controle fornecendo `security-control-id` ou `security-control-arn`.

   Exemplo de comando:

```
aws securityhub --region us-east-1 list-standards-control-associations --
security-control-id Config.1
```

Baixando a lista de controles

É possível baixar a página atual da lista de controles em um arquivo `.csv`.

Se você filtrou a lista de controles, o arquivo baixado incluirá somente os controles que correspondem às configurações do filtro.

Se você escolher um controle específico na lista, o arquivo baixado incluirá somente esse controle.

Para baixar a página atual da lista de controles ou o controle atualmente selecionado, escolha Baixar.

Ativando e desativando controles no padrão

Quando você habilita um padrão no AWS Security Hub, todos os controles que se aplicam a ele são automaticamente habilitados nesse padrão (a exceção são os padrões gerenciados por serviços). Depois, é possível desabilitar e habilitar controles específicos com um padrão habilitado. Entretanto, recomendamos alinhar o status de habilitação de um controle em todos os seus padrões habilitados.

> **Note**
>
> Se você usar a configuração central do Security Hub, o administrador delegado poderá habilitar e desabilitar os controles das contas da organização em todos os padrões habilitados. Recomendamos essa abordagem para que o status de habilitação de um controle esteja alinhado com os padrões. Entretanto, o administrador delegado pode designar contas como autogerenciadas, o que lhes dá a capacidade de habilitar e desabilitar controles em padrões específicos. Para ter mais informações, consulte Como a configuração central funciona.

A página de detalhes de um padrão contém a lista de controles aplicáveis para o padrão e informações sobre quais controles estão atualmente habilitados e desativados nesse padrão.

Na página de detalhes dos padrões, você também pode ativar e desativar controles em um padrão específico. Você deve ativar e desativar os controles separadamente em cada Conta da AWS Região da AWS e. Quando você ativa ou desativa um controle, ele afeta apenas a conta e a região atuais.

Você pode ativar e desativar controles em cada região usando o console do Security Hub, a API do Security Hub ou AWS CLI. Se você definiu uma região de agregação, verá os controles de todas as

regiões vinculadas. Se um controle estiver disponível em uma região vinculada, mas não na região de agregação, você não poderá ativar ou desativar esse controle na região de agregação. Para scripts de desabilitação de controle de várias contas e várias regiões, consulte Desabilitação de controles do Security Hub em um ambiente com várias contas.

Habilitando um controle em um padrão específico

Para ativar um controle em um padrão, você deve primeiro ativar pelo menos um padrão ao qual o controle se aplica. Para obter mais informações sobre ativação de exclusão de MFA, consulte Disabling or enabling a security standard (Desabilitar ou habilitar um padrão de segurança). Quando você ativa um controle em um padrão, AWS Security Hub começa a gerar descobertas para esse controle. O Security Hub inclui o status do controle no cálculo da pontuação de segurança do padrão. Mesmo que você habilite um controle em vários padrões, você receberá uma única descoberta por verificação de segurança em todos os padrões se ativar as descobertas de controle consolidadas. Para obter mais informações, consulte Descobertas de controle consolidadas.

Para ativar um controle em um padrão, o controle deve estar disponível na sua região atual. Para obter mais informações, consulte Disponibilidade de controles por região.

Siga estas etapas para ativar um controle do Security Hub em um padrão específico. Em vez das etapas a seguir, você também pode usar a ação da API `UpdateStandardsControl` para ativar controles em um padrão específico. Para obter instruções sobre como habilitar um controle em todos os padrões, consulte Habilitação de um controle em todos os padrões em uma única conta e região.

Security Hub console

Para habilitar um controle em um padrão específico

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação do , selecione Security standards (Padrões de segurança).
3. Escolha Exibir resultados para um padrão.
4. Selecione um controle.
5. Escolha Ativar controle (essa opção não aparece para um controle que já está ativado). Confirme escolhendo Ativar.

Security Hub API

Para habilitar um controle em um padrão específico

1. Execute `ListSecurityControlDefinitions` e forneça um ARN padrão para obter uma lista dos controles disponíveis para um padrão específico. Para obter o ARN padrão, execute `DescribeStandards`. Essa API retorna IDs de controle de segurança independentes do padrão, não IDs de controle específicos do padrão.

   Exemplo de solicitação

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. Execute `ListStandardsControlAssociations` e forneça um ID de controle específico para retornar o status atual de ativação de um controle em cada padrão.

   Exemplo de solicitação

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. Executar `BatchUpdateStandardsControlAssociations`. Forneça o ARN do padrão no qual você deseja ativar o controle.
4. Defina o parâmetro `AssociationStatus` como `ENABLED`.

   Exemplo de solicitação

   ```
   {
       "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "ENABLED"}]
   }
   ```

AWS CLI

Para habilitar um controle em um padrão específico

1. Execute `list-security-control-definitions` e forneça um ARN padrão para obter uma lista dos controles disponíveis para um padrão específico. Para obter o ARN padrão, execute `describe-standards`. Essa API retorna IDs de controle de segurança independentes do padrão, não IDs de controle específicos do padrão.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Execute `list-standards-control-associations` e forneça um ID de controle específico para retornar o status atual de ativação de um controle em cada padrão.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. Execute o comando `batch-update-standards-control-associations`. Forneça o ARN do padrão no qual você deseja ativar o controle.
4. Defina o parâmetro `AssociationStatus` como `ENABLED`.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]'
```

Habilitando um controle em um padrão específico

Quando você desabilita um controle em um padrão, o Security Hub para de gerar descobertas para o controle. O status do controle não é mais usado no cálculo da pontuação de segurança do padrão.

Uma forma de desativar um controle é desabilitando todos os padrões aos quais o controle se aplica. Quando você desativa um padrão, todos os controles que se aplicam ao padrão são desativados (no entanto, esses controles ainda podem permanecer habilitados em outros padrões). Para obter mais informações sobre como desativar as ACLs, consulte the section called “Habilitar e desabilitar as SCPs”.

Quando você desabilita um controle desativando um padrão ao qual ele se aplica, ocorre o seguinte:

- As verificações de segurança do controle não são mais realizadas para esse padrão. Isso significa que o status do controle não afetará a pontuação de segurança padrão (o Security Hub continuará executando verificações de segurança para o controle se ele estiver ativado em outros padrões).
- Não são geradas descobertas adicionais para esse controle.
- As descobertas existentes para controles desativados são arquivadas automaticamente após três a cinco dias (observe que esse é o melhor esforço e não é garantido).
- As AWS Config regras relacionadas que o Security Hub criou foram removidas.

Além disso, ao desabilitar um padrão inteiro (consulte), o não rastreia quais controles foram desabilitados. Se, depois, você habilitar o padrão novamente, todos os controles serão habilitados. Além disso, desabilitar um controle é uma ação única. Suponha que você desabilite um controle e, em seguida, habilite um padrão que foi desativado anteriormente. Se o padrão incluir esse controle, ele será ativado nesse padrão. Quando você ativa um padrão, o Security Hub ativa automaticamente os controles que se aplicam ao padrão.

Em vez de desativar um controle desativando um padrão ao qual ele se aplica, é possível simplesmente desabilitar o controle em um ou mais padrões específicos.

Para reduzir o ruído de localização, pode ser útil desativar os controles que não são relevantes para o seu ambiente. Para obter recomendações sobre quais controles desabilitar, consulte Controles do Security Hub que você pode querer desabilitar.

Siga estas etapas para desativar um controle em padrões específicos. Em vez das etapas a seguir, você também pode usar a ação da API `UpdateStandardsControl` para ativar controles em um padrão específico. Para obter instruções sobre como habilitar um controle em todos os padrões, consulte .

Security Hub console

Para desabilitar um controle em um padrão específico

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação do , selecione Security standards (Padrões de segurança). Escolha Exibir resultados para um padrão.
3. Selecione um controle.
4. Escolha Ativar controle (essa opção não aparece para um controle que já está ativado).

5. Forneça um motivo para desativar o controle e confirme escolhendo Desativar.

Security Hub API

Para desabilitar um controle em um padrão específico

1. Execute `ListSecurityControlDefinitions` e forneça um ARN padrão para obter uma lista dos controles disponíveis para um padrão específico. Para obter o ARN padrão, execute `DescribeStandards`. Essa API retorna IDs de controle de segurança independentes do padrão, não IDs de controle específicos do padrão.

   Exemplo de solicitação

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. Execute `ListStandardsControlAssociations` e forneça um ID de controle específico para retornar o status atual de ativação de um controle em cada padrão.

   Exemplo de solicitação

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. Executar `BatchUpdateStandardsControlAssociations`. Forneça o ARN do padrão no qual você deseja ativar o controle.
4. Defina o parâmetro `AssociationStatus` como `DISABLED`. Se você seguir essas etapas para um controle que já está desativado, a API retornará uma resposta do código de status HTTP 200.

   Exemplo de solicitação

   ```
   {
       "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "DISABLED",  "UpdatedReason": "Not applicable to environment"}]
   ```

```
}
```

AWS CLI

Para desabilitar um controle em um padrão específico

1. Execute `list-security-control-definitions` e forneça um ARN padrão para obter uma lista dos controles disponíveis para um padrão específico. Para obter o ARN padrão, execute `describe-standards`. Essa API retorna IDs de controle de segurança independentes do padrão, não IDs de controle específicos do padrão.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Execute `list-standards-control-associations` e forneça um ID de controle específico para retornar o status atual de ativação de um controle em cada padrão.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. Execute o comando `batch-update-standards-control-associations`. Forneça o ARN do padrão no qual você deseja ativar o controle.
4. Defina o parâmetro `AssociationStatus` como `DISABLED`. Se você seguir essas etapas para um controle que já está desativado, a API retornará uma resposta do código de status HTTP 200.

```
aws securityhub  --region us-east-1 batch-update-standards-control-
associations --standards-control-association-updates '[{"SecurityControlId":
 "CloudTrail.1", "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "AssociationStatus": "DISABLED",
 "UpdatedReason": "Not applicable to environment"}]'
```

Referência de controles do Security Hub

Essa referência de controles fornece uma lista dos AWS Security Hub controles disponíveis com links para mais informações sobre cada controle. A tabela de visão geral exibe os controles em

ordem alfabética por ID de controle. Somente controles em uso ativo pelo Security Hub estão incluídos aqui. Os controles retirados são excluídos dessa lista. As colunas nesta tabela fornecem as seguintes informações:

- ID de controle de segurança — Essa ID se aplica a todos os padrões AWS service (Serviço da AWS) e indica o recurso ao qual o controle está relacionado. O console do Security Hub exibe IDs de controle de segurança e títulos de controle de segurança, independentemente de as descobertas de controle consolidadas estarem ativadas ou desativadas em sua conta. Entretanto, as descobertas do Security Hub fazem referência aos IDs de controle de segurança somente se as descobertas de controle consolidadas estiverem ativadas em sua conta. Se as descobertas de controle consolidadas estiverem desativadas em sua conta, alguns IDs de controle podem variar de acordo com o padrão em suas descobertas de controle. Para um mapeamento de IDs de controle específicos do padrão para IDs de controle de segurança, consulte Como a consolidação afeta os IDs e títulos de controle.

  Ao configurar automações para controles de segurança, recomendamos filtrar com base no ID do controle, e não no título ou na descrição. Embora o Security Hub possa ocasionalmente atualizar títulos ou descrições de controle, os IDs de controle permanecem os mesmos.

  Os IDs de controle podem ignorar números. Esses são espaços reservados para futuros controles.
- Padrões aplicáveis — Indica a quais padrões um controle se aplica. Selecione um controle para ver os requisitos específicos de estruturas de conformidade de terceiros.
- Título de controle de segurança — Esse título se aplica a todos os padrões. O console do Security Hub exibe IDs de controle de segurança e títulos de controle de segurança, independentemente de as descobertas de controle consolidadas estarem ativadas ou desativadas em sua conta. Entretanto, as descobertas do Security Hub fazem referência aos títulos de controle de segurança somente se as descobertas de controle consolidadas estiverem ativadas em sua conta. Se as descobertas de controle consolidadas estiverem desativadas em sua conta, alguns títulos de controle podem variar de acordo com o padrão em suas descobertas de controle. Para um mapeamento de IDs de controle específicos do padrão para IDs de controle de segurança, consulte Como a consolidação afeta os IDs e títulos de controle.
- Severidade — A severidade de um controle identifica sua importância do ponto de vista da segurança. Para obter informações sobre como o Security Hub determina a severidade do controle, consulte Atribuir severidade às descobertas de controle.
- Tipo de programação — Indica quando o controle é avaliado. Para ter mais informações, consulte Programar a execução de verificações de segurança.

- Oferece suporte a parâmetros personalizados: indica se o controle oferece suporte a valores personalizados para um ou mais parâmetros. Selecione um controle para ver os detalhes dos parâmetros. Para ter mais informações, consulte Parâmetros de controle personalizados.

Selecione uma conexão para visualizar seus detalhes. Os controles são listados em ordem alfabética do nome do serviço.

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
Conta 1	As informações de contato de segurança devem ser fornecidas para um Conta da AWS	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Periódico
Conta 2	Conta da AWS deve fazer parte de uma AWS Organizations organização	NIST SP 800-53 (Revisão 4)	HIGH (ALTO)	 Nº	Periódico
ACM.1	Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Sim	Acionado por alterações e periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
ACM.1	Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits	AWS Melhores práticas básicas de segurança v1.0.0	HIGH (ALTO)	Nº	Acionado por alterações
ACM.3	Os certificados ACM devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
APIGateway.1	O API Gateway, o WebSocket REST e o registro de execução da API devem estar habilitados	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Sim	Acionado por alterações
APIGateway.1	Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
APIGateway.1	API Gateway: os estágios da API REST devem ter AWS X-Ray o rastreamento ativado	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	Baixo	 Nº	Acionado por alterações
APIGateway.1	O API Gateway deve ser associado a uma ACL da web do WAF	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
APIGateway.1	Os dados do cache da API REST de Gateway devem ser criptografados em repouso	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
APIGateway.1	As rotas do API de Gateway devem especificar um tipo de autorização	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Sim	Periódico
APIGateway.1	O registro de acesso deve ser configurado para os estágios V2 do API de Gateway	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
AppSync.2	AWS AppSync deve ter o registro em nível de campo ativado	AWS Melhores práticas básicas de segurança v1.0.0	médio	 Sim	Acionado por alterações
AppSync.4	AWS AppSync As APIs do GraphQL devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
AppSync5.	AWS AppSync As APIs do GraphQL não devem ser autenticadas com chaves de API	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ALTO)	 Nº	Acionado por alterações
Atena.2	Os catálogos de dados do Athena devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
Atena.3	Os grupos de trabalho do Athena devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
AutoScaling.1	Grupos de Auto Scaling associados a um balanceador de carga devem usar verificações de integridade do ELB	AWS Melhores práticas básicas de segurança, padrão gerenciado por serviços: PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	Baixo	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
AutoScaling.2	Grupos e zonas de disponibilidade do Amazon EC2 Auto Scaling	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Sim	Acionado por alterações
AutoScaling.3	As configurações de lançamento em grupo do Auto Scaling devem configurar as instâncias do EC2 para que exijam o Instance Metadata Service versão 2 (IMDSv2)	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	Nº	Acionado por alterações
Auto Scaling	As instâncias do Amazon EC2 lançadas usando as configurações de execução em grupo do Auto Scaling não devem ter endereços IP públicos	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
AutoScaling.6	Os grupos do Auto Scaling devem usar vários tipos de instância em várias zonas de disponibilidade	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
AutoScaling9.	Os grupos do EC2 Auto Scaling devem usar modelos de lançamento do EC2	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
AutoScaling.10	Os grupos do EC2 Auto Scaling devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
Backup.1	AWS Backup os pontos de recuperação devem ser criptografados em repouso	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
Backup.2	AWS Backup os pontos de recuperação devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
Backup.3	AWS Backup cofres devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
Cópia de segurança.4	AWS Backup os planos de relatórios devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
Cópia de segurança.4	AWS Backup planos de backup devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
CloudFormation.2	CloudFormation as pilhas devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
CloudFront.1	CloudFront as distribuições devem ter um objeto raiz padrão configurado	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ALTO)	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
CloudFront.3	CloudFront distribuições devem exigir criptografia em trânsito	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
CloudFront.4	CloudFront as distribuições devem ter o failover de origem configurado	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	Baixo	Nº	Acionado por alterações
CloudFront.5.	CloudFront as distribuições devem ter o registro ativado	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
CloudFront.6	CloudFront as distribuições devem ter o WAF ativado	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
CloudFront.7.	CloudFront as distribuições devem usar certificados SSL/TLS personalizados	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
CloudFront.8.	CloudFront distribuições devem usar SNI para atender solicitações HTTPS	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	Baixo	Nº	Acionado por alterações
CloudFront.9.	CloudFront as distribuições devem criptografar o tráfego para origens personalizadas	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
CloudFront.10	CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
CloudFront.12	CloudFront distribuições não devem apontar para origens inexistentes do S3	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ALTO)	Nº	Periódico
CloudFront.13	CloudFront as distribuições devem usar o controle de acesso de origem	AWS Melhores práticas básicas de segurança v1.0.0	médio	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
CloudFront1.4	CloudFront distribuições devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
CloudTrail.1	CloudTrail deve ser habilitado e configurado com pelo menos uma trilha multirregional que inclua eventos de gerenciamento de leitura e gravação	CIS AWS Foundations Benchmark v1.2.0, CIS Foundations Benchmark v1.4.0, AWS AWS Foundational Security Best Practices v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ALTO)	 Nº	Periódico
CloudTrail.2	CloudTrail deve ter a criptografia em repouso ativada	CIS AWS Foundations Benchmark v1.2.0, Melhores práticas de segurança AWS básicas v1.0.0, Padrão gerenciado por serviços:, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5 AWS	médio	 Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
CloudTrail.3	Pelo menos uma CloudTrail trilha deve ser ativada	PCI DSS v3.2.1	HIGH (ALTO)	Nº	Periódico
CloudTrail.4	CloudTrail a validação do arquivo de log deve ser ativada	CIS AWS Foundations Benchmark v1.2.0, Melhores práticas de segurança AWS básicas v1.0.0, Padrão gerenciado por serviços:, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5 AWS	Baixo	Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
CloudTrail.5.	CloudTrail as trilhas devem ser integradas ao Amazon CloudWatch Logs	CIS AWS Foundations Benchmark v1.2.0, Melhores práticas de segurança AWS básicas v1.0.0, Padrão gerenciado por serviços:, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5 AWS	Baixo	 Nº	Periódico
CloudTrail.6	Certifique-se de que o bucket do S3 usado para armazenar CloudTrail registros não esteja acessível ao público	Referência do CIS AWS Foundations v1.2.0, Referência do CIS Foundations v1.4.0 AWS	Critical	 Nº	Acionado por alterações e periódico
CloudTrail.7.	Certifique-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrail S3	Referência do CIS AWS Foundations v1.2.0, Referência do CIS Foundations v1.4.0 AWS	Baixo	 Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
CloudTrail9.	CloudTrail trilhas devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
CloudWatch.1	Um filtro de métrica de log e um alarme devem existir para uso do usuário “raiz”	Referência do CIS AWS Foundations v1.2.0, PCI DSS v3.2.1, Referência do CIS Foundations v1.4.0 AWS	Baixo	Nº	Periódico
CloudWatch.2	Verificar se existe um alarme e um filtro de métrica de log para chamadas de API não autorizadas	Referência do CIS AWS Foundations v1.2.0	Baixo	Nº	Periódico
CloudWatch.3	Verificar se existe um alarme e um filtro de métrica de log para login do Management Console sem MFA	Referência do CIS AWS Foundations v1.2.0	Baixo	Nº	Periódico
CloudWatch.4	Verificar se existe um alarme e um filtro de métrica de log para alterações de política do IAM	Referência do CIS AWS Foundations v1.2.0, Referência do CIS Foundations v1.4.0 AWS	Baixo	Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
CloudWatch.5.	Certifique-se de que exista um filtro métrico de registro e um alarme para alterações CloudTrail de configuração	Referência do CIS AWS Foundations v1.2.0, Referência do CIS Foundations v1.4.0 AWS	Baixo	Nº	Periódico
CloudWatch.6	Certifique-se de que exista um filtro métrico de registro e um alarme para falhas AWS Management Console de autenticação	Referência do CIS AWS Foundations v1.2.0, Referência do CIS Foundations v1.4.0 AWS	Baixo	Nº	Periódico
CloudWatch.7.	Verificar se existe um alarme e um filtro de métrica de log para a desativação ou exclusão programada de CMKs criadas pelo cliente	Referência do CIS AWS Foundations v1.2.0, Referência do CIS Foundations v1.4.0 AWS	Baixo	Nº	Periódico
CloudWatch.8.	Verificar se existe um alarme e um filtro de métrica de log para alterações de política do bucket do S3	Referência do CIS AWS Foundations v1.2.0, Referência do CIS Foundations v1.4.0 AWS	Baixo	Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
CloudWatch9.	Certifique-se de que exista um filtro métrico de registro e um alarme para alterações AWS Config de configuração	Referência do CIS AWS Foundations v1.2.0, Referência do CIS Foundations v1.4.0 AWS	Baixo	Nº	Periódico
CloudWatch.10	Verificar se existe um alarme e um filtro de métrica de log para alterações do grupo de segurança	Referência do CIS AWS Foundations v1.2.0, Referência do CIS Foundations v1.4.0 AWS	Baixo	Nº	Periódico
CloudWatch1.1	Verificar se existe um alarme e um filtro de métrica de log para alterações em listas de controle de acesso à rede (NACL)	Referência do CIS AWS Foundations v1.2.0, Referência do CIS Foundations v1.4.0 AWS	Baixo	Nº	Periódico
CloudWatch1.2	Verificar se existe um alarme e um filtro de métrica de log para alterações nos gateways de rede	Referência do CIS AWS Foundations v1.2.0, Referência do CIS Foundations v1.4.0 AWS	Baixo	Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
CloudWatch1.3	Verificar se existe um alarme e um filtro de métrica de log para alterações da tabela de rotas	Referência do CIS AWS Foundations v1.2.0, Referência do CIS Foundations v1.4.0 AWS	Baixo	Nº	Periódico
CloudWatch1.4	Verificar se existe um alarme e um filtro de métrica de log para alterações de VPC	Referência do CIS AWS Foundations v1.2.0, Referência do CIS Foundations v1.4.0 AWS	Baixo	Nº	Periódico
CloudWatch1.5	CloudWatch os alarmes devem ter ações especificadas configuradas	NIST SP 800-53 (Revisão 4)	HIGH (ALTO)	Sim	Acionado por alterações
CloudWatch1.6	CloudWatch os grupos de registros devem ser mantidos por um período de tempo especificado	NIST SP 800-53 (Revisão 4)	médio	Sim	Periódico
CloudWatch1.7	CloudWatch ações de alarme devem ser ativadas	NIST SP 800-53 (Revisão 4)	HIGH (ALTO)	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
CodeArtifact.1	CodeArtifact repositórios devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
CodeBuild.1	CodeBuild Os URLs do repositório de origem do Bitbucket não devem conter credenciais confidenciais	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	Critical	Nº	Acionado por alterações
CodeBuild.2	CodeBuild as variáveis de ambiente do projeto não devem conter credenciais de texto não criptografado	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	Critical	Nº	Acionado por alterações
CodeBuild.3	CodeBuild Os registros do S3 devem ser criptografados	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	Baixo	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
CodeBuild.4	CodeBuild ambientes de projeto devem ter uma configuração de registro	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
Config.1	AWS Config deve ser habilitado	CIS AWS Foundations Benchmark v1.2.0, Melhores práticas de segurança AWS básicas v1.0.0, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5 AWS	médio	 Nº	Periódico
DataFirehose.1	Os fluxos de entrega do Firehose devem ser criptografados em repouso	AWS Melhores práticas básicas de segurança NIST SP 800-53 Rev. 5	médio	 Nº	Periódico
Detetive.1	Gráficos de comportamento de Detective devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
DMS.1	As instâncias de replicação do Database Migration Service não devem ser públicas	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	Critical	 Nº	Periódico
DMS.2	Os certificados DMS devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
DMS.3	As assinaturas de eventos do DMS devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
DMS.4	As instâncias de replicação do DMS devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
DMS.5	Os grupos de sub-redes de replicação do DMS devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
DMS.1	As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	 Nº	Acionado por alterações
DMS.1	As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	 Nº	Acionado por alterações
DMS.1	As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	 Nº	Acionado por alterações
DMS.1	Os endpoints do DMS devem usar SSL	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
DMS.10	Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
DMS.11	Os endpoints do DMS para MongoDB devem ter um mecanismo de autenticação habilitado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
DMS.12	Os endpoints do DMS para Redis devem ter o TLS ativado	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
DocumentDB	Os clusters do Amazon DocumentDB devem ser criptografados em repouso	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5, Padrão gerenciado por serviços: AWS Control Tower	médio	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
DocumentDB	Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5, Padrão gerenciado por serviços: AWS Control Tower	médio	Sim	Acionado por alterações
DocumentDB	Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	Critical	Nº	Acionado por alterações
DocumentDB	Os clusters do Amazon DocumentDB devem publicar registros de auditoria em Logs CloudWatch	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
DocumentDB	Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
DynamoDB 2	As tabelas do DynamoDB devem escalar automaticamente a capacidade de acordo com a demanda	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Sim	Periódico
DynamoDB 2	As tabelas do DynamoDB devem ter a recuperação ativada point-in-time	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
DynamoDB 2	Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	 Nº	Periódico
DynamoDB 2	As tabelas do DynamoDB devem estar presentes em um plano de backup	NIST SP 800-53 (Revisão 4)	médio	 Sim	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
DynamoDB 5	As tabelas do DynamoDB devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
DynamoDB 6	As tabelas do DynamoDB devem ter a proteção contra exclusão habilitada	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
DynamoDB 7	Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	médio	Nº	Periódico
EC2.1	[PCI.EC2.1] Os instantâneos do não devem ser restauráveis publicamente	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	Critical	Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
EC2.2	Os grupos de segurança padrão da VPC não devem permitir o tráfego de entrada e saída	CIS AWS Foundations Benchmark v1.2.0, Melhores práticas de segurança AWS básicas v1.0.0, Padrão gerenciado por serviços:, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5 AWS	HIGH (ALTO)	 Nº	Acionado por alterações
EC2.3	[EC2.3] Os volumes anexados do EBS devem ser criptografados em repouso.	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
EC2.4	As instâncias EC2 interrompidas devem ser removidas após um período de tempo especificado	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Sim	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
EC2.6	O registro em de fluxo de VPC deve ser ativado em todas as VPCs	CIS AWS Foundations Benchmark v1.2.0, Melhores práticas de segurança AWS básicas v1.0.0, Padrão gerenciado por serviços:, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5 AWS	médio	Nº	Periódico
EC2.7	A criptografia padrão do EBS deve estar ativada	AWS Melhores práticas básicas de segurança v1.0.0, Padrão gerenciado por serviços:, CIS AWS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5	médio	Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
EC2.8	As instâncias do EC2 devem usar o Instance Metadata Service Version 2 (IMDSv2)	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	 Nº	Acionado por alterações
EC2.9	As instâncias do EC2 não devem ter um endereço IPv4 público	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	 Nº	Acionado por alterações
EC2.10	O Amazon EC2 deve ser configurado para usar endpoints da VPC criados para o serviço Amazon EC2	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Periódico
EC2.12	Os EIPs do EC2 não utilizados devem ser removidos	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	Baixo	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
EC2.13	Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 na porta 22	Referência do CIS AWS Foundations v1.2.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	HIGH (ALTO)	 Nº	Acionado por alterações
EC2.14	Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou: :/0 na porta 3389	Referência do CIS AWS Foundations v1.2.0	HIGH (ALTO)	 Nº	Acionado por alterações
EC2.15	As sub-redes do EC2 não devem atribuir automaticamente endereços IP públicos	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
EC2.16	As listas de controle de acesso à rede não utilizadas devem ser removidas	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	Baixo	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
EC2.17	As instâncias do EC2 não devem usar vários ENIs	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	Baixo	 Nº	Acionado por alterações
EC2.18	Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	 Sim	Acionado por alterações
EC2.19	Grupos de segurança não devem permitir acesso irrestrito a portas com alto risco	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	Critical	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
EC2.20	Ambos os túneis VPN de uma conexão VPN AWS Site-to-Site devem estar ativos	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
EC2.21	As ACLs de rede não devem permitir a entrada de 0.0.0.0/0 para a porta 22 ou porta 3389	AWS Melhores práticas básicas de segurança v1.0.0, Padrão gerenciado por serviços:, CIS AWS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
EC2.22	[PCI.EC2.3] Os grupos de segurança do EC2 devem ser removidos	Padrão gerenciado por serviços: AWS Control Tower	médio	Nº	Periódico
EC2.23	Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ALTO)	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
EC2.24	Os tipos de instância paravirtual do EC2 não devem ser usados	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	 Nº	Acionado por alterações
EC2.25	Os modelos de lançamento do EC2 não devem atribuir IPs públicos às interfaces de rede	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	 Nº	Acionado por alterações
EC2.28	Os volumes do EBS devem estar em um plano de backup	NIST SP 800-53 (Revisão 4)	Baixo	 Sim	Periódico
EC2.33	Os anexos do EC2 Transit Gateway devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EC2.34	As tabelas de rotas do gateway de trânsito EC2 devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
EC2.35	As interfaces de rede EC2 devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EC2.36	Os gateways de clientes do EC2 devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EC2.37	Os endereços IP elásticos do EC2 devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EC2.38	As instâncias do EC2 devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EC2.39	Os gateways de internet EC2 devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EC2.40	Os gateways NAT do EC2 devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
EC2.41	As ACLs de rede EC2 devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EC2.42	As tabelas de rotas do EC2 devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EC2.43	Os grupos de segurança do EC2 devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EC2.44	As sub-redes EC2 devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EC2.45	Os volumes do EC2 devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EC2.46	As Amazon VPCs devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
EC2.47	Os serviços de endpoint do Amazon VPC devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EC2.48	Os registros de fluxo da Amazon VPC devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EC2.49	As conexões de emparelhamento do Amazon VPC devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EC2.50	Os gateways EC2 VPN devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EC2.51	Os endpoints da Client VPN do EC2 devem ter o registro em log de conexão do cliente habilitado	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	Baixo	 Nº	Acionado por alterações
EC2.52	Os gateways de trânsito EC2 devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
EC2.53	Os grupos de segurança do EC2 não devem permitir a entrada de 0.0.0.0/0 para portas de administração de servidores remotos	Referência do CIS AWS Foundations v3.0.0	HIGH (ALTO)	Nº	Periódico
EC2.54	Os grupos de segurança do EC2 não devem permitir a entrada de: :/0 nas portas de administração do servidor remoto	Referência do CIS AWS Foundations v3.0.0	HIGH (ALTO)	Nº	Periódico
ECR.2	Os repositórios privados do ECR devem ter a digitalização de imagens configurada	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
ECR.2	Os repositórios privados do ECR devem ter a digitalização de imagens configurada	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
ECR.2	Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
ECR.4	Os repositórios públicos do ECR devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
ECS.12	As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário.	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
ECS.12	Os serviços do ECS não devem ter endereços IP públicos atribuídos a eles automaticamente	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	Nº	Acionado por alterações
ECS.12	As definições de tarefas do ECS não devem compartilhar o namespace do processo do host	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	Nº	Acionado por alterações
ECS.12	Os contêineres ECS devem ser executados sem privilégios	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
ECS.12	Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	 Nº	Acionado por alterações
ECS.12	Os segredos não devem ser passados como variáveis de ambiente do contêiner	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	 Nº	Acionado por alterações
ECS.12	As definições de tarefas do ECS devem ter uma configuração de registro em log	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ALTO)	 Nº	Acionado por alterações
ECS.12	Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
ECS.12	Os clusters do ECS devem usar Container Insights	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
ECS.13	Os serviços do ECS devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
ECS.14	Os clusters do ECS devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
ECS.15	As definições de tarefas do ECS devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EFS.3	O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
EFS.3	Os volumes do Amazon EBS devem estar em um plano de backup	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Periódico
EFS.3	Os pontos de acesso do EFS devem impor um diretório raiz	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
EFS.3	Os pontos de acesso do EFS devem impor uma identidade de usuário	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
EFS.5	Os pontos de acesso do EFS devem ser marcados	AWS Padrão de marcação de recursos	Baixo	 Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
EFS.6	Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública	AWS Melhores práticas básicas de segurança	médio	Nº	Periódico
eks.1	Os endpoints do cluster EKS não devem ser acessíveis ao público	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ALTO)	Nº	Periódico
eks.2	Os clusters EKS devem ser executados em uma versão compatível do Kubernetes	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	Nº	Acionado por alterações
EKS.3	Os clusters EKS devem usar segredos criptografados do Kubernetes	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	médio	Nº	Periódico
EKS.6	Os clusters EKS devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
EKS.7	As configurações do provedor de identidade EKS devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EKS.8	Os clusters do EKS devem ter o registro em log de auditoria habilitado	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Periódico
ElastiCache.1	ElastiCache Os clusters Redis devem ter o backup automático ativado	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ALTO)	Sim	Periódico
ElastiCache.2	ElastiCache para clusters de cache do Redis, as atualizações automáticas de versões secundárias devem estar habilitadas	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ALTO)	Nº	Periódico
ElastiCache.3	ElastiCache os grupos de replicação devem ter o failover automático ativado	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
ElastiCache.4	ElastiCache grupos de replicação deveriam ter habilitado encryption-at-rest	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Periódico
ElastiCache5.	ElastiCache grupos de replicação deveriam ter habilitado encryption-in-transit	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Periódico
ElastiCache.6	ElastiCache grupos de replicação de versões anteriores do Redis devem ter o Redis AUTH ativado	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Periódico
ElastiCache7.	ElastiCache os clusters não devem usar o grupo de sub-rede padrão	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ALTO)	Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
ElasticBeanstalk.1	Os ambientes do Elastic Beanstalk devem ter os relatórios de saúde aprimorados habilitados	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	Baixo	 Nº	Acionado por alterações
ElasticBeanstalk.2	As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	 Sim	Acionado por alterações
ElasticBeanstalk.3	O Elastic Beanstalk deve transmitir registros para CloudWatch	AWS Melhores práticas básicas de segurança v1.0.0	HIGH (ALTO)	 Sim	Acionado por alterações
ELB.1	O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	médio	 Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
ELB.1	Os Classic Load Balancers com receptores SSL/HTTPS devem usar um certificado fornecido pelo AWS Certificate Manager	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
ELB.1	Os receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
ELB.1	O Application Load Balancer deve ser configurado para eliminar cabeçalhos http	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
ELB.1	O registro em log do Classic Load Balancer e Application Load Balancer deve estar ativado	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
ELB.1	Os balanceadores de carga de aplicativos, gateways e redes devem ter a proteção contra exclusão ativada	AWS Melhores práticas básicas de segurança, padrão gerenciado por serviços: AWS Control Tower, NIST SP 800-53 Rev. 5	médio	 Nº	Acionado por alterações
ELB.1	Os Classic Load Balancers devem ter a drenagem da conexão ativada	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
ELB.1	Os Classic Load Balancers com receptores SSL devem usar uma política de segurança predefinida que tenha uma configuração forte	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
ELB.1	Os Classic Load Balancers devem ter o balanceador de carga entre zonas habilitado	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
ELB.1	Verifica se o Classic Load Balancer abrange várias zonas de disponibilidade (AZs).	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
ELB.1	O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
ELB.1	Balanceadores de carga de aplicações, redes e gateways não abrangem várias zonas de disponibilidade	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Sim	Acionado por alterações
ELB.1	O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
ELB.1	Os balanceadores de carga de aplicativos devem ser associados a uma ACL AWS WAF da web	NIST SP 800-53 (Revisão 4)	médio	 Nº	Acionado por alterações
EMR.1	Os nós primários do cluster Amazon EMR não devem ter endereços IP públicos	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	 Nº	Periódico
EMR.2	A configuração de bloqueio de acesso público do Amazon EMR deve estar habilitada	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	Critical	 Nº	Periódico
ES.1	Os domínios do Elasticsearch devem ter a criptografia em repouso habilitada	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	médio	 Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
ES.2	Os domínios do Elasticsearch não devem ser publicamente acessíveis	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	Critical	 Nº	Periódico
ES.1	Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
ES.1	O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
ES.1	Os domínios do Elasticsearch devem ter o registro em log de auditoria ativado	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
ES.1	Os domínios do Elasticsearch devem ter pelo menos três nós de dados	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
ES.1	Os domínios do Elasticsearch devem ser configurados com pelo menos três nós principais dedicados	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
ES.1	As conexões com os domínios do Elasticsearch devem ser criptografadas usando a política de segurança TLS mais recente	AWS Melhores práticas básicas de segurança, padrão gerenciado por serviços: AWS Control Tower, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
ES.9	Os domínios do Elasticsearch devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EventBridge.2	EventBridge ônibus de eventos devem ser etiquetados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EventBridge.3	EventBridge os ônibus de eventos personalizados devem ter uma política baseada em recursos anexada	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	Baixo	Nº	Acionado por alterações
EventBridge.4	EventBridge endpoints globais devem ter a replicação de eventos ativada	NIST SP 800-53 (Revisão 4)	médio	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
FSx.1	Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	Baixo	 Nº	Acionado por alterações
FSX.2	Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	Baixo	 Nº	Acionado por alterações
Cola.1	AWS Glue os trabalhos devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
GlobalAccelerator.1	Os aceleradores do Global Accelerator devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
GuardDuty.1	GuardDuty deve ser habilitado	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (ALTO)	 Nº	Periódico
GuardDuty.2	GuardDuty os filtros devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
GuardDuty.3	GuardDuty Os IPsets devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
GuardDuty.4	GuardDuty detectores devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
IAM.1	As políticas do IAM não devem permitir privilégios administrativos completos "*"	CIS AWS Foundations Benchmark v1.2.0, Melhores práticas de segurança AWS básicas v1.0.0, Padrão gerenciado por serviços:, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5 AWS	HIGH (ALTO)	 Nº	Acionado por alterações
IAM.2	Os usuários do IAM não devem ter políticas do IAM anexadas	CIS AWS Foundations Benchmark v1.2.0, Melhores práticas de segurança AWS básicas v1.0.0, Padrão gerenciado por serviços:, PCI DSS v3.2.1, NIST SP 800-53 Rev. AWS Control Tower 5	Baixo	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
IAM.3	As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos	CIS AWS Foundations Benchmark v1.2.0, Melhores práticas de segurança AWS básicas v1.0.0, Padrão gerenciado de serviços:, AWS CIS Foundations Benchmark v1.4.0, NIST SP 800-53 AWS Control Tower Rev. 5	médio	 Nº	Periódico
IAM.4	A chave de acesso do usuário raiz do IAM não deve existir	CIS AWS Foundations Benchmark v1.2.0, Melhores práticas de segurança AWS básicas v1.0.0, Padrão gerenciado por serviços:, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5 AWS	Critical	 Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
IAM.5	A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console	CIS AWS Foundations Benchmark v1.2.0, Melhores práticas de segurança AWS básicas v1.0.0, Padrão gerenciado de serviços:, AWS CIS Foundations Benchmark v1.4.0, NIST SP 800-53 AWS Control Tower Rev. 5	médio	 Nº	Periódico
IAM.6	A MFA de hardware deve estar habilitada para o usuário raiz	CIS AWS Foundations Benchmark v1.2.0, Melhores práticas de segurança AWS básicas v1.0.0, Padrão gerenciado por serviços:, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5 AWS	Critical	 Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
IAM.15	Políticas de senha para usuários do IAM que devem ter configurações fortes	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Sim	Periódico
IAM.8	As credenciais de usuário do IAM não utilizadas devem ser removidas	CIS AWS Foundations Benchmark v1.2.0, Melhores práticas de segurança AWS básicas v1.0.0, Padrão gerenciado por serviços:, PCI DSS v3.2.1, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Periódico
IAM.9	[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz	Referência do CIS AWS Foundations v1.2.0, PCI DSS v3.2.1, Referência do CIS Foundations v1.4.0, NIST SP 800-53 Rev. 5 AWS	Critical	 Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
IAM.10	Políticas de senha para usuários do IAM que devem ter configurações fortes	PCI DSS v3.2.1	médio	 Nº	Periódico
IAM.11	Certifique-se que A política de senha do IAM exija pelo menos uma letra maiúscula	Referência do CIS AWS Foundations v1.2.0	médio	 Nº	Periódico
IAM.12	Certifique-se que a política de senha do IAM exija pelo menos uma letra minúscula	Referência do CIS AWS Foundations v1.2.0	médio	 Nº	Periódico
IAM.13	Certifique-se que política de senha do IAM exija pelo menos um símbolo	Referência do CIS AWS Foundations v1.2.0	médio	 Nº	Periódico
IAM.14	Certifique-se que política de senha do IAM exija pelo menos um número	Referência do CIS AWS Foundations v1.2.0	médio	 Nº	Periódico
IAM.15	Certifique-se que a política de senha do IAM exija um comprimento mínimo de 14 ou mais	Referência do CIS AWS Foundations v1.2.0, Referência do CIS Foundations v1.4.0 AWS	médio	 Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
IAM.16	Certifique-se que a política de senha do IAM impeça a reutilização de senhas	Referência do CIS AWS Foundations v1.2.0, Referência do CIS Foundations v1.4.0 AWS	Baixo	 Nº	Periódico
IAM.17	Certifique-se que a política de senha do IAM expire senhas em até 90 dias ou menos	Referência do CIS AWS Foundations v1.2.0	Baixo	 Nº	Periódico
IAM.18	Garanta que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support	Referência do CIS AWS Foundations v1.2.0, Referência do CIS Foundations v1.4.0 AWS	Baixo	 Nº	Periódico
IAM.19	A MFA deve estar habilitada para todos os usuários do IAM	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	médio	 Nº	Periódico
IAM.15	As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	Baixo	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
IAM.15	As credenciais de usuário do IAM não utilizadas devem ser removidas	Referência do CIS AWS Foundations v1.4.0	médio	Nº	Periódico
EU SOU.23	Os analisadores do IAM Access Analyzer devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EU SOU.24	As funções do IAM devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EU SOU.25	Os usuários do IAM devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
EU SOU.26	Os certificados SSL/TLS expirados gerenciados no IAM devem ser removidos	Referência do CIS AWS Foundations v3.0.0	médio	Nº	Periódico
EU SOU.27	As identidades do IAM não devem ter a AWSCloudShellFullAccess política anexada	Referência do CIS AWS Foundations v3.0.0	médio	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
EU SOU 28	O analisador de acesso externo do IAM Access Analyzer deve estar ativado	Referência do CIS AWS Foundations v3.0.0	HIGH (ALTO)	 Nº	Periódico
IoT.1	AWS IoT Core perfis de segurança devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
IoT.2	AWS IoT Core ações de mitigação devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
IoT.3	AWS IoT Core as dimensões devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
IoT.4	AWS IoT Core os autorizadores devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
IoT.5	AWS IoT Core aliases de função devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
IoT.6	AWS IoT Core as políticas devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
Kinesis.1	Os fluxos do Kinesis devem ser criptografados em repouso	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
Cinesia.2	Os streams do Kinesis devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
KMS.4	As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
KMS.4	As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
KMS.4	AWS KMS keys não deve ser excluído acidentalmente	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	Critical	Nº	Acionado por alterações
KMS.4	AWS KMS key a rotação deve ser ativada	Referência do CIS AWS Foundations v1.2.0, PCI DSS v3.2.1, Referência do CIS Foundations v1.4.0, NIST SP 800-53 Rev. 5 AWS	médio	Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
Lambda.1	As funções do Lambda devem proibir o acesso público	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	Critical	 Nº	Acionado por alterações
Lambda.1	[Lambda.2] As funções do devem usar os tempos de execução mais recentes	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
Lambda.3	As funções do Lambda devem estar em uma VPC	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	Baixo	 Nº	Acionado por alterações
Lambda.5	As funções do Lambda da VPC devem operar em várias zonas de disponibilidade	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
Lambda.6	As funções Lambda devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
Macie.1	O Amazon Macie deve estar ativado	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Periódico
Macie.2	A descoberta automatizada de dados confidenciais do Macie deve ser ativada	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ALTO)	Nº	Periódico
MSK.1	Os clusters MSK devem ser criptografados em trânsito entre os nós do agente	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
MSK.2	Os clusters do MSK devem ter um monitoramento aprimorado configurado	NIST SP 800-53 (Revisão 4)	Baixo	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
MQ.2	Os corretores ActiveMQ devem transmitir os registros de auditoria para CloudWatch	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	médio	 Nº	Acionado por alterações
MQ.3	Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	Baixo	 Nº	Acionado por alterações
MQ.4	Os corretores do Amazon MQ devem ser etiquetados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
MQ.5	Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera	NIST SP 800-53 Rev. 5, padrão gerenciado por serviços: AWS Control Tower	Baixo	 Nº	Acionado por alterações
MQ.5	Os agentes do RabbitMQ devem usar o modo de implantação de cluster	NIST SP 800-53 Rev. 5, padrão gerenciado por serviços: AWS Control Tower	Baixo	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
Neptune.1	Os clusters de banco de dados Neptune devem ser criptografados em repouso	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5, Padrão gerenciado por serviços: AWS Control Tower	médio	 Nº	Acionado por alterações
Neptune.3	Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5, Padrão gerenciado por serviços: AWS Control Tower	médio	 Nº	Acionado por alterações
Neptune.3	Os instantâneos do cluster de banco de dados Neptune não devem ser públicos	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5, Padrão gerenciado por serviços: AWS Control Tower	Critical	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
Neptune.3	Indica se o cluster de banco de dados deve ter a proteção contra exclusão habilitada.	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5, Padrão gerenciado por serviços: AWS Control Tower	Baixo	 Nº	Acionado por alterações
Neptune.3	Os clusters de banco de dados Neptune devem ter backups automatizados habilitados	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5, Padrão gerenciado por serviços: AWS Control Tower	médio	 Sim	Acionado por alterações
Neptune.3	Os clusters de banco de dados Neptune devem ser criptografados em repouso	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5, Padrão gerenciado por serviços: AWS Control Tower	médio	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
Neptune.3	Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5, Padrão gerenciado por serviços: AWS Control Tower	médio	 Nº	Acionado por alterações
Neptune.3	Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5, Padrão gerenciado por serviços: AWS Control Tower	Baixo	 Nº	Acionado por alterações
Neptune.9	Os clusters de banco de dados Neptune devem ser implantados em várias zonas de disponibilidade	NIST SP 800-53 (Revisão 4)	médio	 Nº	Acionado por alterações
NetworkFirewall.1	Os firewalls do Network Firewall devem ser implantados em várias zonas de disponibilidade	NIST SP 800-53 (Revisão 4)	médio	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
NetworkFirewall.2	O registro em log do Network Firewall deve ser habilitado	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Periódico
NetworkFirewall.3	As políticas de Firewall de Rede devem ter pelo menos um grupo de regras associado	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
NetworkFirewall.4	A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar pacotes completos.	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
NetworkFirewall5.	A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar pacotes completos.	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
NetworkFirewall.6	O grupo de regras de firewall de rede sem estado não deve estar vazio	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
NetworkFirewall7.	Firewall de rede (firewalls) devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
NetworkFirewall8.	As políticas de firewall do Network Firewall devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
NetworkFirewall9.	Os firewalls do Firewall de Rede devem ter a proteção contra exclusão ativada	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
Opensearch.1	OpenSearch os domínios devem ter a criptografia em repouso ativada	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
Opensearch.2	OpenSearch os domínios não devem ser acessíveis ao público	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	Critical	Nº	Acionado por alterações
OpenSearch 1.3	OpenSearch os domínios devem criptografar os dados enviados entre os nós	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
OpenSearch 1.3	OpenSearch o registro de erros de domínio CloudWatch nos registros deve estar ativado	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
OpenSearch 1.3	OpenSearch os domínios devem ter o registro de auditoria ativado	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
OpenSearch 1.3	OpenSearch os domínios devem ter pelo menos três nós de dados	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
OpenSearch 1.3	OpenSearch os domínios devem ter um controle de acesso refinado ativado	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	Nº	Acionado por alterações
OpenSearch 1.3	As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente	AWS Melhores práticas básicas de segurança, padrão gerenciado por serviços: AWS Control Tower, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
Pesquisa aberta. 9	OpenSearch domínios devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
Opensearch.10	OpenSearch os domínios devem ter a atualização de software mais recente instalada	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	Baixo	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
Abrir pesquisa. 11	OpenSearch os domínios devem ter pelo menos três nós primários dedicados	NIST SP 800-53 (Revisão 4)	médio	Nº	Periódico
PCA.1	AWS Private CA a autoridade de certificação raiz deve ser desativada	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	Baixo	Nº	Periódico
RDS.1	[RDS.1] Os instantâneos do RDS devem ser privados	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	Critical	Nº	Acionado por alterações
RDS.2	As instâncias de banco de dados do RDS devem proibir o acesso público, conforme determinado pela configuração PubliclyAccessible	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	Critical	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
RDS. 3	As instâncias de banco de dados do RDS devem ter a criptografia em repouso habilitada.	AWS Melhores práticas básicas de segurança v1.0.0, Padrão gerenciado por serviços:, CIS AWS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
RDS. 3	Os instantâneos do cluster do RDS e os instantâneos do banco de dados devem ser criptografados em repouso	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
RDS. 3	As instâncias de banco de dados do RDS devem ser configuradas com várias zonas de disponibilidade	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
RDS. 3	O monitoramento aprimorado deve ser configurado para instâncias de banco de dados do RDS	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	Baixo	 Sim	Acionado por alterações
RDS. 3	Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	Baixo	 Nº	Acionado por alterações
RDS. 3	Indica se a instância de banco de dados deve ter a proteção contra exclusão habilitada.	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	Baixo	 Nº	Acionado por alterações
RDS. 3	As instâncias de banco de dados do RDS devem publicar registros em Logs CloudWatch	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
RDS. 3	A autenticação do IAM deve ser configurada para instâncias do RDS	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
RDS. 3	As instâncias do RDS devem ter backups automáticos habilitados	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Sim	Acionado por alterações
RDS. 3	A autenticação do IAM deve ser configurada para instâncias do RDS	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
RDS. 3	Habilitar atualizações automáticas entre versões secundárias do	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
RDS. 3	O retrocesso do cluster MySQL do Amazon Aurora não está habilitado	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	 Sim	Acionado por alterações
RDS. 3	As instâncias de banco de dados do RDS devem ser configuradas com várias zonas de disponibilidade	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	 Nº	Acionado por alterações
RDS. 3	Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	Baixo	 Nº	Acionado por alterações
RDS. 3	As instâncias de banco de dados do RDS devem ser configuradas para copiar tags para instantâneos	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	Baixo	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
RDS. 3	As instâncias do RDS devem ser implantadas em uma VPC	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	 Nº	Acionado por alterações
RDS. 3	As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de cluster	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	Baixo	 Nº	Acionado por alterações
RDS. 3	As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de cluster	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	Baixo	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
RDS. 3	Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de parâmetros do banco de dados	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	Baixo	Nº	Acionado por alterações
RDS. 3	Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de parâmetros do banco de dados	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	Baixo	Nº	Acionado por alterações
RDS. 3	As instâncias do RDS não devem usar uma porta padrão do mecanismo de banco de dados	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	Baixo	Nº	Acionado por alterações
RDS. 3	Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
RDS. 3	Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
RDS. 3	As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup	NIST SP 800-53 (Revisão 4)	médio	 Sim	Periódico
RDS. 3	Os clusters de banco de dados Neptune devem ser criptografados em repouso	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5, Padrão gerenciado por serviços: AWS Control Tower	médio	 Nº	Acionado por alterações
RDS. 28	Os clusters de banco de dados do RDS devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
RDS. 29	Os instantâneos do cluster de banco de dados do RDS devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
RDS 30	As instâncias de banco de dados do RDS devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
RDS. 31	Os grupos de segurança do banco de dados do RDS devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
RDS. 32	Os instantâneos de banco de dados do RDS devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
RDS. 33	Os grupos de sub-redes do banco de dados do RDS devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
RDS. 3	Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
RDS. 3	Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
Redshift. 1	Os clusters do Amazon Redshift devem proibir o acesso público	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	Critical	Nº	Acionado por alterações
5439 (Redshift)	As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
5439 (Redshift)	Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
Redshift.4	Os clusters do Amazon Redshift devem ter o registro de auditoria ativado	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
Redshift.9	O Amazon Redshift deve ter as atualizações automáticas para as versões principais habilitadas	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
Redshift.9	Os clusters do Redshift devem usar roteamento de VPC aprimorado	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
Redshift.9	Os clusters do Amazon Redshift não devem usar o nome de usuário Admin padrão	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
Redshift.9	Os clusters do Amazon Redshift não devem usar o nome de usuário Admin padrão	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
5439 (Redshift)	Os clusters de banco de dados Neptune devem ser criptografados em repouso	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
Desvio para o vermelho.11	Os clusters do Redshift devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
Desvio para o vermelho. 12	As notificações de assinatura de eventos do Redshift devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
Desvio para o vermelho. 13	Os instantâneos do cluster do Redshift devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
Desvio para o vermelho. 14	Os grupos de sub-redes do cluster Redshift devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
Desvio para o vermelho. 15	Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas	AWS Melhores práticas básicas de segurança	HIGH (ALTO)	 Nº	Periódico
Rota 53.1	As verificações de saúde do Route 53 devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
Route53.2	As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	 Nº	Acionado por alterações
S3.1	Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas	AWS Melhores práticas básicas de segurança, padrão gerenciado por serviços: PCI DSS v3.2.1 AWS Control Tower, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5	médio	 Nº	Periódico
S3.2	Os buckets de uso geral do S3 devem bloquear o acesso público de leitura	AWS Melhores práticas básicas de segurança, padrão gerenciado por serviços: PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	Critical	 Nº	Acionado por alterações e periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
S3.3	Os buckets de uso geral do S3 devem bloquear o acesso público de gravação	AWS Melhores práticas básicas de segurança, padrão gerenciado por serviços: PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	Critical	 Nº	Acionado por alterações e periódico
S3.5	Os buckets de uso geral do S3 devem exigir solicitações para usar SSL	AWS Melhores práticas básicas de segurança, padrão gerenciado por serviços: PCI DSS v3.2.1 AWS Control Tower, CIS AWS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5	médio	 Nº	Acionado por alterações
S3.6	As políticas de bucket de uso geral do S3 devem restringir o acesso a outros Contas da AWS	AWS Melhores práticas básicas de segurança, padrão gerenciado por serviços: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (ALTO)	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
S3.7	Os buckets de uso geral do S3 devem usar a replicação entre regiões	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	Baixo	 Nº	Acionado por alterações
S3.8	Os buckets de uso geral do S3 devem bloquear o acesso público	AWS Melhores práticas básicas de segurança, padrão gerenciado por serviços:, CIS AWS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (ALTO)	 Nº	Acionado por alterações
S3.9	Os buckets de uso geral do S3 devem ter o registro de acesso ao servidor ativado	AWS Melhores práticas básicas de segurança, padrão gerenciado por serviços: AWS Control Tower, NIST SP 800-53 Rev. 5	médio	 Nº	Acionado por alterações
S3.10	Os buckets de uso geral do S3 com versionamento ativado devem ter configurações de ciclo de vida	NIST SP 800-53 (Revisão 4)	médio	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
S3.11	Os buckets de uso geral do S3 devem ter as notificações de eventos ativadas	NIST SP 800-53 (Revisão 4)	médio	Sim	Acionado por alterações
S3.12	As ACLs não devem ser usadas para gerenciar o acesso do usuário aos buckets de uso geral do S3	AWS Melhores práticas básicas de segurança, padrão gerenciado por serviços: AWS Control Tower, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
S3.13	Os buckets de uso geral do S3 devem ter configurações de ciclo de vida	AWS Melhores práticas básicas de segurança, padrão gerenciado por serviços: AWS Control Tower, NIST SP 800-53 Rev. 5	Baixo	Sim	Acionado por alterações
S3.14	Os buckets de uso geral do S3 devem ter o controle de versão ativado	NIST SP 800-53 (Revisão 4)	Baixo	Nº	Acionado por alterações
S3.15	Os buckets de uso geral do S3 devem ter o Object Lock ativado	NIST SP 800-53 (Revisão 4)	médio	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
S3.17	Os buckets de uso geral do S3 devem ser criptografados em repouso com AWS KMS keys	Padrão gerenciado por serviços: AWS Control Tower, NIST SP 800-53 Rev. 5	médio	 Nº	Acionado por alterações
S3.19	Os pontos de acesso do S3 devem ter configurações de bloqueio do acesso público habilitadas	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	Critical	 Nº	Acionado por alterações
S3.20	Os buckets de uso geral do S3 devem ter a exclusão de MFA habilitada	Referência do CIS AWS Foundations v1.4.0, NIST SP 800-53 Rev. 5	Baixo	 Nº	Acionado por alterações
S3.22	Os buckets de uso geral do S3 devem registrar eventos de gravação em nível de objeto	Referência do CIS AWS Foundations v3.0.0	médio	 Nº	Periódico
S3.23	Os buckets de uso geral do S3 devem registrar eventos de leitura em nível de objeto	Referência do CIS AWS Foundations v3.0.0	médio	 Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
SageMaker.1	As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (ALTO)	Nº	Periódico
SageMaker.2	SageMaker instâncias de notebook devem ser lançadas em uma VPC personalizada	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	Nº	Acionado por alterações
SageMaker.3	Os usuários não devem ter acesso root às instâncias do SageMaker notebook	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ALTO)	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
SageMaker.4	SageMaker as variantes de produção de endpoints devem ter uma contagem inicial de instâncias maior que 1	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	médio	Nº	Periódico
SecretsManager.1	Os segredos do Secrets Manager devem ter a alternância automática ativada	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Sim	Acionado por alterações
SecretsManager.2	Os segredos do Secrets Manager configurados com alternância automática devem girar com sucesso	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Nº	Acionado por alterações
SecretsManager.3	Adicionar ou remover segredos do Secrets Manager.	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	Sim	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
SecretsManager.4	Os segredos do Secrets Manager devem ser alternados dentro de um determinado número de dias	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Sim	Periódico
SecretsManager5.	Os segredos do Secrets Manager devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
ServiceCatalog.1	Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma AWS organização	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	HIGH (ALTO)	 Nº	Periódico
SES.1	As listas de contatos do SES devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
SES.2	Os conjuntos de configuração do SES devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
SNS.1	Os tópicos do SNS devem ser criptografados em repouso usando AWS KMS	NIST SP 800-53 (Revisão 4)	médio	 Nº	Acionado por alterações
SNS.3	Os tópicos do SNS devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
SQS.1	As filas do Amazon SQS devem ser criptografadas em repouso	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
SQS.2	As filas SQS devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
SSM.1	As instâncias do EC2 devem ser gerenciadas por AWS Systems Manager	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	médio	Nº	Acionado por alterações
SSM.2	As instâncias do EC2 gerenciadas pelo devem ter um status de conformidade de patch de COMPLIANT após a instalação do patch	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (ALTO)	Nº	Acionado por alterações
SSM.3	As instâncias de EC2 gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	Baixo	Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
SSM.3	Os documentos SSM não devem ser públicos	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	Critical	 Nº	Periódico
StepFunctions.1	As máquinas de estado do Step Functions devem ter o registro ativado	AWS Melhores práticas básicas de segurança	médio	 Sim	Acionado por alterações
StepFunctions.2	As atividades do Step Functions devem ser marcadas	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
Transferência.1	Os fluxos de trabalho do Transfer Family devem ser marcados	AWS Padrão de marcação de recursos	Baixo	Sim	Acionado por alterações
Transferência.2	Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoint	AWS Melhores práticas básicas de segurança, NIST SP 800-53 Rev. 5	médio	 Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
WAF.1	AWS WAF O registro clássico do Global Web ACL deve estar ativado	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	 Nº	Periódico
WAF.6	AWS WAF As regras regionais clássicas devem ter pelo menos uma condição	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
WAF.6	AWS WAF Os grupos de regras regionais clássicos devem ter pelo menos uma regra	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
WAF.6	AWS WAF As ACLs regionais clássicas da web devem ter pelo menos uma regra ou grupo de regras	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
WAF.6	AWS WAF As regras globais clássicas devem ter pelo menos uma condição	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	 Nº	Acionado por alterações
WAF.6	AWS WAF Os grupos de regras globais clássicos devem ter pelo menos uma regra	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	 Nº	Acionado por alterações
WAF.6	AWS WAF As ACLs web globais clássicas devem ter pelo menos uma regra ou grupo de regras	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	 Nº	Acionado por alterações
WAF.6	AWS WAF as ACLs da web devem ter pelo menos uma regra ou grupo de regras	AWS Melhores práticas básicas de segurança v1.0.0, padrão gerenciado por serviços:, NIST SP 800-53 Rev. AWS Control Tower 5	médio	 Nº	Acionado por alterações
WAF.6	AWS WAF o registro de ACL na web deve estar ativado	NIST SP 800-53 (Revisão 4)	Baixo	 Nº	Periódico

ID do controle de segurança	Título de controle de segurança	Padrões aplicáveis	Gravidade	Oferece suporte a parâmetros personalizados	tipo: Schedule
WAF.6	AWS WAF as regras devem ter CloudWatch métricas ativadas	AWS Melhores práticas básicas de segurança v1.0.0, NIST SP 800-53 Rev. 5	médio	 Nº	Acionado por alterações

Tópicos

- Conta da AWS controles
- AWS Certificate Manager controles
- Conceitos do Amazon API Gateway
- AWS AppSync controles
- Controles do Amazon Athena
- AWS Backup controles
- AWS CloudFormation controles
- CloudFront Controles da Amazon
- AWS CloudTrail controles
- CloudWatch Controles da Amazon
- AWS CodeArtifact controles
- AWS CodeBuild controles
- AWS Config controles
- Controles do Amazon Data Firehose
- Controles do Amazon Detective
- AWS Database Migration Service controles
- Controles do Amazon DocumentDB
- Controles do Amazon DynamoDB

- Amazon Elastic Container Registry
- Controlador do Amazon ECS
- Amazon Elastic Compute Cloud - Compute
- Grupo do Amazon EC2 Auto Scaling
- Amazon EC2 Systems Manager
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- ElastiCache Controles da Amazon
- AWS Elastic Beanstalk controles
- Elastic Load Balancing Concepts (Conceitos do Elastic Load Balancing)
- Controles do Amazon EMR
- Controles do Elasticsearch
- EventBridge Controles da Amazon
- Controles do Amazon FSx
- AWS Global Accelerator controles
- AWS Glue controles
- GuardDuty Controles da Amazon
- AWS Identity and Access Management controles
- AWS IoT controles
- Controles do Amazon Kinesis
- AWS Key Management Service controles
- AWS Lambda controles
- Controles do Amazon Macie
- Controles do Amazon EKS
- Controles do Amazon MQ
- Controles do Amazon Neptune
- AWS Network Firewall controles
- Controles OpenSearch do Amazon Service
- AWS Private Certificate Authority controles

- Amazon Relational Database Service
- COPY do Amazon Redshift
- Conceitos do Amazon Route 53
- Amazon Simple Storage Service Batch
- SageMaker Controles da Amazon
- AWS Secrets Manager controles
- AWS Service Catalog controles
- Controles do Amazon Simple Email Service
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- AWS Step Functions controles
- AWS Transfer Family controles
- AWS WAF controles

Conta da AWS controles

Esses controles estão relacionados Contas da AWS a.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[Conta.1] As informações de contato de segurança devem ser fornecidas para um Conta da AWS

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Configuração de recursos

Severidade: média

Tipo de recurso

Regra do AWS Config : `security-account-information-provided`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se uma conta da Amazon Web Services (AWS) tem informações de contato de segurança. O controle falhará se as informações de contato de segurança não forem fornecidas para a conta.

Contatos de segurança alternativos AWS permitem que você entre em contato com outra pessoa sobre problemas com sua conta, caso você não esteja disponível. As notificações podem ser de AWS Support, ou de outras AWS service (Serviço da AWS) equipes, sobre tópicos relacionados à segurança associados ao seu uso. Conta da AWS

Correção

Para adicionar um contato alternativo como contato de segurança ao seu Conta da AWS, consulte Adicionar, alterar ou remover contatos alternativos no Guia do Usuário do AWS Billing and Cost Management.

[A conta.2] Contas da AWS deve fazer parte de uma organização AWS Organizations

Categoria: Proteger > Gerenciamento de acesso seguro

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Severidade: alta

Tipo de recurso

Regra do AWS Config : `account-part-of-organizations`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um Conta da AWS faz parte de uma organização gerenciada por AWS Organizations. O controle falhará se a conta não fizer parte de uma organização.

O Organizations ajuda você a gerenciar centralmente seu ambiente à medida que você expande suas cargas de trabalho. AWSÉ possível usar várias Contas da AWS para isolar workloads que tenham requisitos de segurança específicos ou para cumprir estruturas como HIPAA ou PCI. Ao criar uma organização, você pode administrar várias contas como uma única unidade e gerenciar centralmente seus acessos Serviços da AWS, recursos e regiões.

Correção

Para criar uma nova organização e Contas da AWS adicioná-la automaticamente, consulte Criação de uma organização no Guia do AWS Organizations usuário. Para adicionar contas a uma organização existente, consulte Convidar e Conta da AWS participar da sua organização no Guia do AWS Organizations usuário.

AWS Certificate Manager controles

Esses controles estão relacionados à .

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado

Requisitos relacionados: NIST.800-53.r5 SC-28 (3), NIST.800-53.r5 SC-7 (16)

Categoria: Proteger > Proteção de dados > Criptografia de dados em trânsito

Severidade: média

Tipo de recurso

Regra do AWS Config : `acm-certificate-expiration-check`

Tipo de agendamento: alteração acionada e periódica

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`daysToExpiration`	Número de dias em que o certificado ACM deve ser renovado	Inteiro	`14` para `365`	`30`

Esse controle verifica se um certificado AWS Certificate Manager (ACM) é renovado dentro do período de tempo especificado. Ele verifica os certificados importados e os certificados fornecidos pelo ACM. O controle falhará se o certificado não for renovado dentro do período especificado. A menos que você forneça um valor de parâmetro personalizado para o período de renovação, o Security Hub usará um valor padrão de 30 dias.

O renova automaticamente os certificados do que você validou usando o DNS. Para os certificados que usam validação de email, você deve responder a um email de validação de domínio. O ACM não renovará automaticamente os certificados que você importar. É necessário renovar certificados importados manualmente.

Correção

O ACM fornece renovação gerenciada para seus certificados SSL/TLS emitidos pela Amazon. Isso significa que o ACM renovará seus certificados automaticamente (se você estiver usando a validação por DNS) ou enviará avisos por email quando a expiração da validade estiver se aproximando. Esses serviços são fornecidos para certificados públicos e privados do ACM.

Renovação de domínios validados por email

Quando um certificado está a 45 dias da expiração, o ACM envia ao proprietário do domínio um email para cada nome de domínio. Para validar os domínios e concluir a renovação, você deve responder às notificações por email.

Para obter mais informações, consulte Renovação de domínios validados por email no Guia do usuário do AWS Certificate Manager .

Renovação de domínios validados pelo DNS

O ACM renova automaticamente os certificados que usam a validação de DNS. 60 dias antes da expiração, o ACM verifica se o certificado pode ser renovado.

Se não puder validar um nome de domínio, o ACM enviará uma notificação de que a validação manual é necessária. O envia essas notificações 45 dias, 30 dias, 7 dias e 1 dia antes da expiração da validade.

Para obter mais informações, consulte validação de DNS no no Guia do usuário AWS Certificate Manager .

Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits

Categoria: Identificar > Inventário > Serviços de inventário

Severidade: alta

Tipo de recurso

Regra do AWS Config : `acm-certificate-rsa-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os certificados RSA gerenciados por AWS Certificate Manager usam um comprimento de chave de pelo menos 2.048 bits. O controle falhará se o comprimento da chave for menor que 2.048 bits.

A força da criptografia se correlaciona diretamente com o tamanho da chave. Recomendamos tamanhos de chave de pelo menos 2.048 bits para proteger seus AWS recursos à medida que a capacidade de computação se torna mais barata e os servidores se tornam mais avançados.

Correção

O tamanho mínimo da chave para certificados RSA emitidos pelo ACM já é de 2.048 bits. Para obter instruções sobre a emissão de novos certificados RSA com o ACM, consulte Emissão e gerenciamento de certificados no Guia do usuário do AWS Certificate Manager .

Embora o ACM permita importar certificados com tamanhos de chave mais curtos, você deve usar chaves de pelo menos 2.048 bits para passar por esse controle. Não é possível alterar o tamanho da chave após a importação de um certificado. Em vez disso, você deve excluir certificados com um tamanho de chave menor que 2.048 bits. Para obter mais informações sobre a importação de certificados de terceiros para o ACM, consulte Importação de certificados no Guia do usuário do AWS Certificate Manager .

[ACM.3] Os certificados ACM devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-acm-certificate` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um certificado AWS Certificate Manager (ACM) tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o certificado não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o certificado não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder

à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um certificado ACM, consulte Como marcar AWS Certificate Manager certificados no Guia do AWS Certificate Manager usuário.

Conceitos do Amazon API Gateway

Esses controles estão relacionados aos recursos da API de Gateway.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[ApiGateway.1] O REST do API Gateway WebSocket e o registro de execução da API devem estar habilitados

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `api-gw-execution-logging-enabled`

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`loggingLevel`	Nível de registro	Enum	`ERROR`, `INFO`	`No default value`

Esse controle verifica se todos os estágios de uma REST ou API do Amazon WebSocket API Gateway têm o registro ativado. O controle falhará se o `loggingLevel` não for `ERROR` ou `INFO` em todos os estágios da API. A menos que você forneça valores de parâmetros personalizados para indicar que um tipo de log específico deve ser habilitado, o Security Hub produzirá uma descoberta aprovada se o nível de registro em log for `ERROR` ou `INFO`.

Os estágios REST ou WebSocket API do API Gateway devem ter os registros relevantes habilitados. O REST do WebSocket API Gateway e o registro de execução da API fornecem registros detalhados das solicitações feitas nos estágios REST e WebSocket API do API Gateway. Os estágios incluem respostas de back-end de integração de API, respostas do autorizador Lambda e `requestId` endpoints de integração for. AWS

Correção

Para ativar o registro em log para operações de WebSocket REST e API, consulte Configurar o registro de CloudWatch API usando o console do API Gateway no Guia do desenvolvedor do API Gateway.

Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados

Severidade: média

Tipo de recurso

Regra do AWS Config : `api-gw-ssl-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os estágios da API REST do Amazon API Gateway têm certificados SSL configurados. Os sistemas de back-end usam esses certificados para autenticar que as solicitações recebidas são da API Gateway.

Os estágios da API REST da API Gateway devem ser configurados com certificados SSL para permitir que os sistemas de back-end autentiquem que as solicitações são originadas da API Gateway.

Correção

Para obter instruções detalhadas sobre como gerar e configurar certificados SSL da API REST da API Gateway, consulte Gerar e configurar um certificado SSL para autenticação de back-end no Guia do desenvolvedor do API Gateway.

Os estágios da API REST de Gateway devem ter o rastreamento AWS X-Ray habilitado.

Requisitos relacionados: NIST.800-53.r5 CA-7

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `api-gw-xray-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o rastreamento AWS X-Ray ativo está habilitado para os estágios da API REST do Amazon API Gateway.

O rastreamento ativo X-Ray permite uma resposta mais rápida às alterações de desempenho na infraestrutura subjacente. Alterações no desempenho podem resultar na falta de disponibilidade da

API. O rastreamento ativo do X-Ray fornece métricas em tempo real das solicitações do usuário que fluem pelas operações da API REST da API Gateway e serviços conectados.

Correção

Para obter instruções detalhadas sobre como habilitar o rastreamento ativo do X-Ray para operações de API REST do API Gateway, consulte o suporte ao rastreamento ativo do Amazon API Gateway para AWS X-Ray no Guia do desenvolvedor do AWS X-Ray .

O API Gateway deve ser associado a uma WAF Web ACL

Requisitos relacionados: NIST.800-53.r5 CA-7

Categoria: Proteger > Serviços de proteção

Severidade: média

Tipo de recurso

Regra do AWS Config : `api-gw-associated-with-waf`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um estágio do API Gateway usa uma lista de controle de acesso à AWS WAF web (ACL). Esse controle falhará se uma AWS WAF Web ACL não estiver conectada a um estágio do REST API Gateway.

AWS WAF é um firewall de aplicativos da web que ajuda a proteger aplicativos e APIs da web contra ataques. Isso permite configurar um conjunto de regras chamado de lista de controle de acesso à web (ACL da web) que permitem, bloqueiam ou contam solicitações da web com base em regras e condições de segurança da web personalizáveis que você define. Certifique-se de que seu estágio do API Gateway esteja associado a uma ACL AWS WAF da web para ajudar a protegê-lo contra ataques maliciosos.

Correção

Para obter informações sobre como usar o console do API Gateway para associar uma ACL da web AWS WAF regional a um estágio de API do API Gateway existente, consulte Como usar AWS WAF para proteger suas APIs no Guia do desenvolvedor do API Gateway.

Os dados do cache da API REST de Gateway devem ser criptografados em repouso

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra AWS Config : `api-gw-cache-encrypted` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se todos os métodos nos estágios da API REST do API Gateway que têm o cache ativado estão criptografados. O controle falhará se algum método em um estágio da API REST do API Gateway estiver configurado para armazenar em cache e o cache não estiver criptografado. O Security Hub atualizou o controle para avaliar a criptografia de um método específico somente quando o armazenamento em cache estiver habilitado para esse método.

Criptografar dados em repouso reduz o risco de os dados armazenados em disco serem acessados por um usuário não autenticado. AWS Ele adiciona outro conjunto de controles de acesso para limitar a capacidade de usuários não autorizados acessarem os dados. Por exemplo, as permissões da API são necessárias para descriptografar os dados antes que eles possam ser lidos.

Os caches da API REST do API Gateway devem ser criptografados em repouso para uma camada adicional de segurança.

Correção

Para configurar o cache da API para um estágio, consulte Habilitar o armazenamento em cache do Amazon API Gateway no Guia do desenvolvedor do API Gateway. Em Configurações de cache, escolha Criptografar dados de cache.

As rotas do API de Gateway devem especificar um tipo de autorização

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

AWS Config regra: `api-gwv2-authorization-type-configured`

Tipo de programação: Periódico

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`authorizationType`	Tipo de autorização das rotas de API	Enum	`AWS_IAM`, `CUSTOM`, `JWT`	Nenhum valor padrão

Esse controle verifica se as rotas do Amazon API Gateway têm um tipo de autorização. O controle falhará se a rota do API Gateway não tiver nenhum tipo de autorização. Opcionalmente, é possível fornecer um valor de parâmetro personalizado se quiser que o controle passe somente se a rota usar o tipo de autorização especificado no parâmetro `authorizationType`.

O API Gateway oferece suporte a vários mecanismos de controle e gerenciamento de acesso à sua API. Ao especificar um tipo de autorização, é possível restringir o acesso à sua API somente a usuários ou processos autorizados.

Correção

Para definir um tipo de autorização para APIs HTTP, consulte Controlar e gerenciar o acesso a uma API HTTP no API Gateway no Guia do desenvolvedor do API Gateway. Para definir um tipo de autorização para WebSocket APIs, consulte Controle e gerenciamento do acesso a uma WebSocket API no API Gateway no Guia do desenvolvedor do API Gateway.

O registro de acesso deve ser configurado para os estágios V2 do API de Gateway

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

AWS Config regra: `api-gwv2-access-logs-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os estágios do Amazon API Gateway V2 têm o registro em log de acesso configurado. Esse controle falhará se as configurações do log de acesso não estiverem definidas.

Os logs de acesso ao API Gateway fornecem informações detalhadas sobre quem acessou sua API e como o chamador acessou a API. Esses logs são úteis para aplicações como auditorias de segurança e acesso e investigação forense. Habilite esses logs de acesso para analisar padrões de tráfego e solucionar problemas.

Para obter mais práticas recomendadas, consulte Monitoramento de APIs REST no Guia do desenvolvedor do API Gateway.

Correção

Para configurar o registro de acesso, consulte Configurar o registro de CloudWatch API usando o console do API Gateway no Guia do desenvolvedor do API Gateway.

AWS AppSync controles

Esses controles estão relacionados aos AWS AppSync recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `appsync-logging-enabled`

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub	
`fieldLoggingLevel`	Nível de registro em log de campo	Enum	`ERROR`, `ALL`	No `default value`	

Esse controle verifica se uma AWS AppSync API tem o registro em nível de campo ativado. O controle falhará se o nível do log do resolvedor de campo estiver definido como Nenhum. A menos que você forneça valores de parâmetros personalizados para indicar que um tipo de log específico deve ser habilitado, o Security Hub produzirá uma descoberta aprovada se o nível de log do resolvedor de campo for `ERROR` ou `ALL`.

É possível usar o registro em log e as métricas para identificar, solucionar problemas e otimizar as consultas do GraphQL. Ativar o registro no AWS AppSync GraphQL ajuda você a obter informações detalhadas sobre solicitações e respostas de API, identificar e responder a problemas e cumprir os requisitos regulatórios.

Correção

Para ativar o registro em log AWS AppSync, consulte Instalação e configuração no Guia do AWS AppSync desenvolvedor.

[AppSync.4] As APIs AWS AppSync do GraphQL devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-appsync-graphqlapi` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se uma API do AWS AppSync GraphQL tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se a API GraphQL não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro. `requiredTagKeys` Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a API GraphQL não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive

AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma API do AWS AppSync GraphQL, consulte TagResourcena Referência da AWS AppSync API.

[AppSync.5] As APIs AWS AppSync do GraphQL não devem ser autenticadas com chaves de API

Requisitos relacionados: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6

Categoria: Proteger > Gerenciamento de acesso seguro > Autenticação sem senha

Severidade: alta

Tipo de recurso

Regra do AWS Config : `appsync-authorization-check`

Tipo de programação: acionado por alterações

Parâmetros:

- `AllowedAuthorizationTypes: AWS_LAMBDA, AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS` (não personalizável)

Esse controle verifica se seu aplicativo usa uma chave de API para interagir com uma API do AWS AppSync GraphQL. O controle falhará se uma API do AWS AppSync GraphQL for autenticada com uma chave de API.

Uma chave de API é um valor codificado em seu aplicativo que é gerado pelo AWS AppSync serviço quando você cria um endpoint GraphQL não autenticado. Se essa chave de API for comprometida, seu endpoint ficará vulnerável ao acesso não intencional. A menos que você ofereça suporte a um aplicativo ou site acessível ao público, não recomendamos o uso de uma chave de API para autenticação.

Correção

Para definir uma opção de autorização para sua API do AWS AppSync GraphQL, consulte Autorização e autenticação no Guia do AWS AppSync desenvolvedor.

Controles do Amazon Athena

Esses controles estão relacionados aos recursos da API de Gateway.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

Os grupos de trabalho do Athena devem ser criptografados em repouso

> **Important**
>
> O Security Hub retirou esse controle em abril de 2024. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Severidade: média

Tipo de recurso

Regra do AWS Config : `athena-workgroup-encrypted-at-rest`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um grupo de trabalho do Athena está criptografado em repouso. Esse controle verifica se um grupo de trabalho do Athena está criptografado em repouso.

No Athena, é possível criar grupos de trabalho para executar consultas para equipes, aplicativos ou workloads diferentes. Cada grupo de trabalho tem uma configuração para ativar a criptografia

em todas as consultas. Você tem a opção de usar criptografia do lado do servidor com chaves gerenciadas do Amazon Simple Storage Service (Amazon S3), criptografia do lado do servidor com chaves AWS KMS() ou criptografia do lado do cliente AWS Key Management Service com chaves KMS gerenciadas pelo cliente. Dados em repouso se referem a qualquer dado armazenado em armazenamento persistente e não volátil por qualquer período. A criptografia ajuda a proteger a confidencialidade desses dados, reduzindo o risco de que um usuário não autorizado possa acessá-los.

Correção

Para habilitar a criptografia em repouso para grupos de trabalho do Athena, consulte Editar um grupo de trabalho no Guia do usuário do Amazon Athena. Na seção Configuração do resultado da consulta, selecione Criptografar resultados da consulta.

[Athena.2] Os catálogos de dados do Athena devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-athena-datacatalog` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um catálogo de dados do Amazon Athena tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o catálogo de dados não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o catálogo de dados não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um catálogo de dados do Athena, consulte Como marcar recursos do Athena no Guia do usuário do Amazon Athena.

[Athena.3] Os grupos de trabalho do Athena devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-athena-workgroup` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um grupo de trabalho do Amazon Athena tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o grupo de trabalho não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o grupo de trabalho não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um grupo de trabalho do Athena, consulte Adicionar e excluir tags em um grupo de trabalho individual no Guia do usuário do Amazon Athena.

AWS Backup controles

Esses controles estão relacionados aos AWS Backup recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso

Requisitos relacionados: NIST.800-53.r5 CP-9(8), NIST.800-53.r5 SI-12

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso

Regra do AWS Config : `backup-recovery-point-encrypted`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um ponto AWS Backup de recuperação está criptografado em repouso. O controle falhará se o ponto de recuperação não estiver criptografado em repouso.

Um ponto de AWS Backup recuperação se refere a uma cópia ou instantâneo específico dos dados que é criado como parte de um processo de backup. Ele representa um momento específico em que

o backup dos dados foi feito e serve como um ponto de restauração caso os dados originais sejam perdidos, corrompidos ou fiquem inacessíveis. Criptografar os pontos de recuperação de backup adicionará uma camada extra de proteção contra acesso não autorizado. A criptografia é uma prática recomendada para proteger a confidencialidade, a integridade e a segurança dos dados de backup.

Correção

Para criptografar um ponto AWS Backup de recuperação, consulte Criptografia para backups AWS Backup no Guia do AWS Backup desenvolvedor.

[Backup.2] os pontos de AWS Backup recuperação devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config: `tagged-backup-recoverypoint` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um ponto de AWS Backup recuperação tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o ponto de

recuperação não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o ponto de recuperação não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um ponto AWS Backup de recuperação

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, selecione Planos de backup.
3. Selecione um plano de backup na lista.
4. Na seção Tags do plano de backup, escolha Gerenciar tags.
5. Insira a chave e o valor da tag. Escolha Adicionar nova tag para pares de valores-chave adicionais.
6. Quando terminar de adicionar tags, selecione Save (Salvar).

[Backup.3] os AWS Backup cofres devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config: `tagged-backup-backupvault` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um AWS Backup cofre tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o ponto de recuperação não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o ponto de recuperação não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags.

Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um AWS Backup cofre

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, selecione Cofres de Backup.
3. Selecione um cofre de backup na lista.
4. Na seção Backup de tags do cofre, escolha Gerenciar tags.
5. Insira a chave e o valor da tag. Escolha Adicionar nova tag para pares de valores-chave adicionais.
6. Quando terminar de adicionar tags, selecione Save (Salvar).

[Backup.4] os planos de AWS Backup relatórios devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config: `tagged-backup-reportplan` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um plano de AWS Backup relatório tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o plano de relatório não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o plano de relatório não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive

AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um plano de AWS Backup relatório

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, selecione Cofres de Backup.
3. Selecione um cofre de backup na lista.
4. Na seção Backup de tags do cofre, escolha Gerenciar tags.
5. Selecione Adicionar nova tag. Insira a chave e o valor da tag. Repita o procedimento para pares adicionais de valores-chave.
6. Quando terminar de adicionar tags, selecione Save (Salvar).

[Backup.5] os planos de AWS Backup backup devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config: `tagged-backup-backupplan` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o	StringList	Lista de tags que atendem	Nenhum valor padrão

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.		aos AWS requisitos	

Esse controle verifica se um plano de AWS Backup backup tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o plano de backup não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o plano de backup não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um plano AWS Backup de backup

1. Abra o AWS Backup console em https://console.aws.amazon.com/backup.
2. No painel de navegação, selecione Cofres de Backup.
3. Selecione um cofre de backup na lista.
4. Na seção Backup de tags do cofre, escolha Gerenciar tags.
5. Selecione Adicionar nova tag. Insira a chave e o valor da tag. Repita o procedimento para pares adicionais de valores-chave.
6. Quando terminar de adicionar tags, selecione Save (Salvar).

AWS CloudFormation controles

Esses controles estão relacionados aos CloudFormation recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[CloudFormation.1] CloudFormation as pilhas devem ser integradas ao Simple Notification Service (SNS)

> **Important**
>
> O Security Hub retirou esse controle em abril de 2024. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Requisitos relacionados: NIST.800-53.r5 SI-4 (12), NIST.800-53.r5 SI-4 (5)

Categoria: Detectar > Serviços de detecção > Monitoramento de aplicativos

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `cloudformation-stack-notification-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma notificação do Amazon Simple Notification Service está integrada a uma pilha do AWS CloudFormation . O controle falhará em uma CloudFormation pilha se nenhuma notificação do SNS estiver associada a ela.

Configurar uma notificação do SNS com sua CloudFormation pilha ajuda a notificar imediatamente as partes interessadas sobre quaisquer eventos ou alterações que ocorram com a pilha.

Correção

Para integrar uma CloudFormation pilha e um tópico do SNS, consulte Atualização de pilhas diretamente no Guia do AWS CloudFormation usuário.

[CloudFormation.2] as CloudFormation pilhas devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-cloudformation-stack` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se uma AWS CloudFormation pilha tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a pilha não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a pilha não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma CloudFormation pilha, consulte CreateStackna Referência da AWS CloudFormation API.

CloudFront Controles da Amazon

Esses controles estão relacionados aos CloudFront recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado

Requisitos relacionados: NIST.800-53.r5 SC-28 (3), NIST.800-53.r5 SC-7 (16)

Categoria: Proteger > Gerenciamento de acesso seguro > Recursos não acessíveis ao público

Severidade: alta

Tipo de recurso

Regra do AWS Config : `cloudfront-default-root-object-configured`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma CloudFront distribuição da Amazon está configurada para retornar um objeto específico que é o objeto raiz padrão. O controle falhará se a CloudFront distribuição não tiver um objeto raiz padrão configurado.

Às vezes, um usuário pode solicitar a URL raiz da distribuição em vez de um objeto na distribuição. Quando isso acontece, a especificação de um objeto raiz padrão pode ajudá-lo a evitar a exposição do conteúdo da sua distribuição da web.

Correção

Para configurar um objeto raiz padrão para uma CloudFront distribuição, consulte Como especificar um objeto raiz padrão no Amazon CloudFront Developer Guide.

[CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em trânsito

Severidade: média

Tipo de recurso

Regra do AWS Config : `cloudfront-viewer-policy-https`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma CloudFront distribuição da Amazon exige que os espectadores usem HTTPS diretamente ou se ela usa redirecionamento. O controle falhará se `ViewerProtocolPolicy` estiver definido como `allow-all` para `defaultCacheBehavior` ou para`cacheBehaviors`.

O HTTPS (TLS) pode ser usado para ajudar a impedir que possíveis invasores usem ataques semelhantes para espionar person-in-the-middle ou manipular o tráfego da rede. Somente conexões criptografadas por HTTPS (TLS) devem ser permitidas. A criptografia de dados em trânsito pode afetar o desempenho. Você deve testar seu aplicativo com esse atributo para entender o perfil de desempenho e o impacto do TLS.

Correção

Para criptografar uma CloudFront distribuição em trânsito, consulte Exigir HTTPS para comunicação entre espectadores e CloudFront no Amazon CloudFront Developer Guide.

[CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `cloudfront-origin-failover-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma CloudFront distribuição da Amazon está configurada com um grupo de origem que tem duas ou mais origens.

CloudFront o failover de origem pode aumentar a disponibilidade. Se a origem primária estiver indisponível ou retornar códigos de status de resposta HTTP específicos que indiquem falha, o failover automaticamente alternará para a origem secundária.

Correção

Para configurar o failover de origem para uma CloudFront distribuição, consulte Criação de um grupo de origem no Amazon CloudFront Developer Guide.

[CloudFront.5] CloudFront as distribuições devem ter o registro ativado

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `cloudfront-accesslogs-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o registro de acesso ao servidor está habilitado nas CloudFront distribuições. O controle falhará se o registro em log de acesso não estiver habilitado para uma distribuição.

CloudFront os registros de acesso fornecem informações detalhadas sobre cada solicitação do usuário que CloudFront recebe. Cada log contém informações como a data e a hora em que a solicitação foi recebida, o endereço IP do visualizador que fez a solicitação, a origem da solicitação e o número da porta da solicitação do visualizador.

Esses logs são úteis para aplicações como auditorias de segurança e acesso e investigação forense. Para obter orientações adicionais sobre como analisar registros de acesso, consulte Consultar CloudFront registros da Amazon no Guia do usuário do Amazon Athena.

Correção

Para configurar o registro de acesso para uma CloudFront distribuição, consulte Configuração e uso de registros padrão (registros de acesso) no Amazon CloudFront Developer Guide.

[CloudFront.6] as CloudFront distribuições devem ter o WAF ativado

Requisitos relacionados: NIST.800-53.r5 CA-7

Categoria: Proteger > Serviços de proteção

Severidade: média

Tipo de recurso

Regra do AWS Config : `cloudfront-associated-with-waf`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se CloudFront as distribuições estão associadas às ACLs AWS WAF clássicas ou AWS WAF da web. O controle falhará se a distribuição não estiver associada a uma ACL da web.

AWS WAF é um firewall de aplicativos da web que ajuda a proteger aplicativos e APIs da web contra ataques. Isso permite configurar um conjunto de regras chamado de lista de controle de acesso à web (ACL da web) que permitem, bloqueiam ou contam solicitações da web com base em regras e condições de segurança da web personalizáveis que você define. Certifique-se de que sua CloudFront distribuição esteja associada a uma ACL AWS WAF da web para ajudar a protegê-la contra ataques maliciosos.

Correção

Para associar uma ACL AWS WAF da web a uma CloudFront distribuição, consulte Usando AWS WAF para controlar o acesso ao seu conteúdo no Amazon CloudFront Developer Guide.

[CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3),

NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso

Regra do AWS Config : `cloudfront-custom-ssl-certificate`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se CloudFront as distribuições estão usando o certificado SSL/TLS padrão fornecido. CloudFront Esse controle passa se a CloudFront distribuição usa um certificado SSL/TLS personalizado. Esse controle falhará se a CloudFront distribuição usar o certificado SSL/TLS padrão.

O SSL/TLS personalizado permite que seus usuários acessem o conteúdo usando nomes de domínio alternativos. É possível armazenar certificados personalizados no AWS Certificate Manager (recomendado) ou no IAM.

Correção

Para adicionar um nome de domínio alternativo para uma CloudFront distribuição usando um certificado SSL/TLS personalizado, consulte Adicionar um nome de domínio alternativo no Amazon CloudFront Developer Guide.

[CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Proteger > Configuração de rede segura

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `cloudfront-sni-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se CloudFront as distribuições da Amazon estão usando um certificado SSL/TLS personalizado e estão configuradas para usar o SNI para atender solicitações HTTPS. Esse controle falhará se um certificado SSL/TLS personalizado estiver associado, mas o método de suporte SSL/TLS for um endereço IP dedicado.

A Indicação de nome de servidor (SNI) é uma extensão do protocolo TLS, compatível com os navegadores e clientes lançados após 2010. Se você configurar CloudFront para atender solicitações HTTPS usando SNI, CloudFront associe seu nome de domínio alternativo a um endereço IP para cada ponto de presença. Quando um visualizador envia uma solicitação HTTPS para seu conteúdo, o DNS a roteia para o endereço IP do ponto de presença correto. O endereço IP para o seu nome de domínio é determinado durante a negociação do handshake SSL/TLS. O endereço IP não é dedicado à sua distribuição.

Correção

Para configurar uma CloudFront distribuição para usar o SNI para atender às solicitações HTTPS, consulte Como usar o SNI para atender às solicitações HTTPS (funciona para a maioria dos clientes) no Guia do CloudFront desenvolvedor.

[CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso

Regra do AWS Config : `cloudfront-traffic-to-origin-encrypted`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se CloudFront as distribuições da Amazon estão criptografando o tráfego para origens personalizadas. Esse controle falha em uma CloudFront distribuição cuja política de protocolo de origem permite “somente http”. Esse controle também falhará se a política do protocolo de origem da distribuição for “match-viewer”, enquanto a política do protocolo do visualizador for “allow-all”.

O HTTPS (TLS) pode ser usado para ajudar a evitar a espionagem ou a manipulação do tráfego da rede. Somente conexões criptografadas por HTTPS (TLS) devem ser permitidas.

Correção

Para atualizar a Política do Protocolo de Origem para exigir criptografia para uma CloudFront conexão, consulte Exigir HTTPS para comunicação entre CloudFront e sua origem personalizada no Amazon CloudFront Developer Guide.

[CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso

Regra do AWS Config : `cloudfront-no-deprecated-ssl-protocols`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se CloudFront as distribuições da Amazon estão usando protocolos SSL obsoletos para comunicação HTTPS entre pontos de presença e suas CloudFront origens personalizadas. Esse controle falhará se uma CloudFront distribuição tiver um `CustomOriginConfig` where `OriginSslProtocols` includes`SSLv3`.

Em 2015, a Internet Engineering Task Force (IETF) anunciou oficialmente que o SSL 3.0 deveria ser descontinuado devido ao protocolo não ser suficientemente seguro. É recomendável usar o TLSv1.2 ou posterior para comunicação HTTPS com suas origens personalizadas.

Correção

Para atualizar os protocolos SSL de origem para uma CloudFront distribuição, consulte Exigir HTTPS para comunicação entre CloudFront e sua origem personalizada no Amazon CloudFront Developer Guide.

[CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Configuração de recursos

Severidade: alta

Tipo de recurso

Regra do AWS Config : `cloudfront-s3-origin-non-existent-bucket`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se CloudFront as distribuições da Amazon estão apontando para origens inexistentes do Amazon S3. O controle falhará em uma CloudFront distribuição se a origem estiver configurada para apontar para um bucket inexistente. Esse controle se aplica somente às CloudFront distribuições em que um bucket do S3 sem hospedagem estática do site é a origem do S3.

Quando uma CloudFront distribuição em sua conta é configurada para apontar para um bucket inexistente, um terceiro mal-intencionado pode criar o bucket referenciado e veicular seu próprio conteúdo por meio de sua distribuição. Recomendamos verificar todas as origens, independentemente do comportamento de roteamento, para garantir que suas distribuições estejam apontando para as origens apropriadas.

Correção

Para modificar uma CloudFront distribuição para apontar para uma nova origem, consulte Atualização de uma distribuição no Amazon CloudFront Developer Guide.

[CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem

Categoria: Proteger > Gerenciamento de acesso seguro > Configuração da política de recursos

Severidade: média

Tipo de recurso

Regra do AWS Config : `cloudfront-s3-origin-access-control-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma CloudFront distribuição da Amazon com origem no Amazon S3 tem controle de acesso de origem (OAC) configurado. O controle falhará se o OAC não estiver configurado para a CloudFront distribuição.

Ao usar um bucket do S3 como origem para sua CloudFront distribuição, você pode ativar o OAC. Isso permite o acesso ao conteúdo no bucket somente por meio da CloudFront distribuição especificada e proíbe o acesso diretamente do bucket ou de outra distribuição. Embora CloudFront ofereça suporte ao Origin Access Identity (OAI), o OAC oferece funcionalidades adicionais e as distribuições que usam o OAI podem migrar para o OAC. Embora o OAI forneça uma maneira segura de acessar as origens do S3, ele tem limitações, como a falta de suporte para configurações de políticas granulares e para solicitações HTTP/HTTPS que usam o método POST, pois exigem a AWS Signature Version 4 (SigV4). Regiões da AWS O OAI também não oferece suporte à criptografia com AWS Key Management Service. O OAC é baseado em uma prática AWS recomendada de uso de entidades de serviço do IAM para autenticar com origens do S3.

Correção

Para configurar o OAC para uma CloudFront distribuição com origens do S3, consulte Restringir o acesso a uma origem do Amazon S3 no Amazon Developer Guide. CloudFront

[CloudFront.14] as CloudFront distribuições devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

AWS Config regra: `tagged-cloudfront-distribution` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se uma CloudFront distribuição da Amazon tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a distribuição não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a distribuição não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma CloudFront distribuição, consulte Como marcar CloudFront distribuições da Amazon no Amazon CloudFront Developer Guide.

AWS CloudTrail controles

Esses controles estão relacionados aos CloudTrail recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[CloudTrail.1] CloudTrail deve ser habilitado e configurado com pelo menos uma trilha multirregional que inclua eventos de gerenciamento de leitura e gravação

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/2.1, CIS Foundations Benchmark v1.4.0/3.1, CIS AWS Foundations Benchmark v3.0.0/3.1, NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10 800-53.R5 AU-12, NiST.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NISt.800-53.R5 AU-6 (3), NISt.800-53.R5 AU-6 (4), NIST.800-53.R5 AU-14 (1), NISt.800-53.R5 CA-7, NIST.800-53.R5 R5 SC-7 (9), Nist.800-53.R5 SI-3 (8), NIST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-7 (8), NIST.800-53.R5 SA-8 (22) AWS

Categoria: Identificar > Registro em log

Severidade: alta

Tipo de recurso

Regra do AWS Config : `multi-region-cloudtrail-enabled`

Tipo de programação: Periódico

Parâmetros:

- `readWriteType`: `ALL` (não personalizável)

  `includeManagementEvents`: `true` (não personalizável)

Esse controle verifica se há pelo menos uma AWS CloudTrail trilha multirregional que captura eventos de gerenciamento de leitura e gravação. O controle falhará se CloudTrail estiver desativado ou se não houver pelo menos uma CloudTrail trilha que capture eventos de gerenciamento de leitura e gravação.

AWS CloudTrail registra chamadas de AWS API para sua conta e entrega arquivos de log para você. As informações registradas incluem as seguintes informações:

- Identidade do chamador da API
- Hora da chamada da API
- Endereço IP de origem do chamador da API
- Parâmetros de solicitação
- Elementos de resposta retornados pelo AWS service (Serviço da AWS)

CloudTrail fornece um histórico de chamadas de AWS API para uma conta, incluindo chamadas de API feitas a partir das ferramentas de linha de comando AWS Management Console, AWS SDKs. O histórico também inclui chamadas de API de nível superior Serviços da AWS , como. AWS CloudFormation

O histórico de chamadas da AWS API produzido por CloudTrail permite análise de segurança, rastreamento de alterações de recursos e auditoria de conformidade. As trilhas de várias regiões também oferecem os seguintes benefícios.

- A trilha de várias regiões ajuda a detectar atividades inesperadas que ocorram em regiões não utilizadas de outra forma.
- Uma trilha de várias regiões garante que o registro em log de eventos do serviço global esteja habilitado para uma trilha por padrão. O registro global de eventos de serviços registra eventos gerados por serviços AWS globais.
- Para uma trilha multirregional, os eventos de gerenciamento de todas as operações de leitura e gravação garantem que as operações de gerenciamento de CloudTrail registros em todos os recursos em uma Conta da AWS.

Por padrão, as CloudTrail trilhas criadas usando o AWS Management Console são trilhas multirregionais.

Correção

Para criar uma nova trilha multirregional em CloudTrail, consulte Criação de uma trilha no Guia do AWS CloudTrail usuário. Use os seguintes valores:

Campo	Valor
Configurações adicionais, validação do arquivo de log	Habilitado
Escolha eventos de logs, eventos de gerenciamento, atividade de API	Ler e Gravar. Desmarque as caixas de seleção para exclusões.

Para atualizar uma trilha existente, consulte Atualizar uma trilha no Guia do usuário do AWS CloudTrail . Em Eventos de gerenciamento, para Atividade da API, escolha Ler e Gravar.

[CloudTrail.2] CloudTrail deve ter a criptografia em repouso ativada

Requisitos relacionados: PCI DSS v3.2.1/3.4, CIS Foundations Benchmark v1.2.0/2.7, CIS Foundations Benchmark v1.4.0/3.7, CIS AWS Foundations Benchmark v3.0.0/3.5, NIST.800-53.r5 AU-9, NIST.800-53.r5 AWS CA-9 (1), NIST.800-53.r5 AWS CM-3 (6), NIST.800-53.r5 3.r5 SC-13, Nist.800-53.R5 SC-28, NIST.800-53.R5 SC-28 (1), Nist.800-53.R5 SC-7 (10), Nist.800-53.R5 SI-7 (6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra do AWS Config : `cloud-trail-encryption-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se CloudTrail está configurado para usar a criptografia de criptografia do lado do servidor (SSE). AWS KMS key O controle falha se `KmsKeyId` não estiver definido.

Para uma camada adicional de segurança para seus arquivos de CloudTrail log confidenciais, você deve usar criptografia do lado do servidor com AWS KMS keys (SSE-KMS) para seus arquivos de CloudTrail log para criptografia em repouso. Observe que, por padrão, os arquivos de log entregues CloudTrail aos seus buckets são criptografados pela criptografia do lado do servidor da Amazon com chaves de criptografia gerenciadas pelo Amazon S3 (SSE-S3).

Correção

Para ativar a criptografia SSE-KMS para arquivos de CloudTrail log, consulte Atualizar uma trilha para usar uma chave KMS no Guia do usuário.AWS CloudTrail

[CloudTrail.3] Pelo menos uma CloudTrail trilha deve ser ativada

Requisitos relacionados: PCI DSS v3.2.1/10.1, PCI DSS v3.2.1/10.2.1, PCI DSS v3.2.1/10.2.2, PCI DSS v3.2.1/10.2.3, PCI DSS v3.2.1/10.2.4, PCI DSS v3.2.1/10.2.5, PCI DSS v3.2.1/10.2.6, PCI DSS v3.2.1/10.2.7, PCI DSS v3.2.1/10.3.1, PCI DSS v3.2.1/10.3.2, PCI DSS v3.2.1/10.3.3, PCI DSS v3.2.1/10.3.4, PCI DSS v3.2.1/10.3.5, PCI DSS v3.2.1/10.3.6

Categoria: Identificar > Registro em log

Severidade: alta

Tipo de recurso

Regra do AWS Config : `cloudtrail-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se uma AWS CloudTrail trilha está habilitada no seu Conta da AWS. O controle falhará se sua conta não tiver pelo menos uma CloudTrail trilha ativada.

No entanto, alguns AWS serviços não permitem o registro de todas as APIs e eventos. Você deve implementar quaisquer trilhas de auditoria adicionais além de CloudTrail revisar a documentação de cada serviço em Serviços e Integrações CloudTrail Suportados.

Correção

Para começar CloudTrail e criar uma trilha, consulte o AWS CloudTrail tutorial Introdução no Guia do AWS CloudTrail usuário.

[CloudTrail.4] a validação do arquivo de CloudTrail log deve estar ativada

Requisitos relacionados: PCI DSS v3.2.1/10.5.2, PCI DSS v3.2.1/10.5.5, CIS Foundations Benchmark v1.2.0/2.2, CIS Foundations Benchmark v1.4.0/3.2, CIS AWS Foundations Benchmark v3.0.0/3.2, NIST.800-53.r5 AU-9, NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-7 (1), AWS Nist.800-53.R5 SI-7 (3), Nist.800-53.R5 AWS SI-7 (7)

Categoria: Proteção de dados > Integridade dos dados

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `cloud-trail-log-file-validation-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se a validação da integridade do arquivo de log está habilitada em uma CloudTrail trilha.

CloudTrail a validação do arquivo de log cria um arquivo de resumo assinado digitalmente que contém um hash de cada log CloudTrail gravado no Amazon S3. Você pode usar esses arquivos de resumo para determinar se um arquivo de log foi alterado, excluído ou inalterado após a CloudTrail entrega do log.

Recomendamos que você ative a validação de arquivos em todas as trilhas. A validação do arquivo de log fornece verificações adicionais de integridade dos CloudTrail registros.

Correção

Para ativar a validação do arquivo de CloudTrail log, consulte Habilitando a validação da integridade do arquivo de log CloudTrail no Guia AWS CloudTrail do usuário.

[CloudTrail.5] CloudTrail trilhas devem ser integradas com o Amazon CloudWatch Logs

Requisitos relacionados: PCI DSS v3.2.1/10.5.3, CIS Foundations Benchmark v1.2.0/2.4, CIS AWS Foundations Benchmark v1.4.0/3.4, NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26),

NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10 Nist.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-6 (1), NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NISt.800-53.R5 AU-6 (5), Nist.800-53.R5 AU-7 (1), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NiST.800-53.R5 SI-20, NIST.800-53.R5 SI-3 (8), NiST.800-53.R5 SI-4 (20), NIST.800-53.R5 SI-4 (AWS 5), NIST.800-53.R5 SI-7 (8)

Categoria: Identificar > Registro em log

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `cloud-trail-cloud-watch-logs-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se as CloudTrail trilhas estão configuradas para enviar registros para o CloudWatch Logs. O controle falhará se a propriedade `CloudWatchLogsLogGroupArn` da trilha estiver vazia.

CloudTrail registra as chamadas de AWS API feitas em uma determinada conta. A solicitação inclui as seguintes informações:

- Identidade do chamador da API
- Hora da chamada da API
- Endereço IP de origem do chamador da API
- Mapear parâmetros de solicitação
- Os elementos de resposta retornados pelo AWS service (Serviço da AWS)

CloudTrail usa o Amazon S3 para armazenamento e entrega de arquivos de log. Você pode capturar CloudTrail registros em um bucket S3 especificado para análise de longo prazo. Para realizar análises em tempo real, você pode configurar o CloudTrail envio de registros para o CloudWatch Logs.

Para uma trilha ativada em todas as regiões de uma conta, CloudTrail envia arquivos de registro de todas essas regiões para um grupo de CloudWatch registros de registros.

O Security Hub recomenda que você envie CloudTrail registros para o CloudWatch Logs. Observe que essa recomendação tem como objetivo garantir que a atividade da conta seja capturada, monitorada e devidamente alertada. Você pode usar o CloudWatch Logs para configurar isso com seu Serviços da AWS. Essa recomendação não impede o uso de uma solução diferente.

O envio de CloudTrail CloudWatch registros para o Logs facilita o registro histórico e em tempo real de atividades com base no usuário, na API, no recurso e no endereço IP. Ele fornece a oportunidade de estabelecer alertas e notificações de atividades anormais ou confidenciais da conta.

Correção

Para fazer a integração CloudTrail com o CloudWatch Logs, consulte Enviar eventos para o CloudWatch Logs no Guia AWS CloudTrail do usuário.

[CloudTrail.6] Certifique-se de que o bucket do S3 usado para armazenar CloudTrail registros não esteja acessível ao público

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/2.3, CIS Foundations Benchmark v1.4.0/3.3 AWS

Categoria: Identificar > Registro em log

Severidade: crítica

Tipo de recurso

AWS Config regra: Nenhuma (regra personalizada do Security Hub)

Tipo de programação: periódico e acionado por alterações

Parâmetros: nenhum

CloudTrail registra um registro de cada chamada de API feita em sua conta. Esses arquivos de log são armazenados em um bucket do S3. O CIS recomenda que a política de bucket do S3, ou lista de controle de acesso (ACL), seja aplicada ao bucket do S3 que CloudTrail registra para impedir o acesso público aos registros. CloudTrail Permitir o acesso público ao conteúdo do CloudTrail registro pode ajudar um adversário a identificar pontos fracos no uso ou na configuração da conta afetada.

Para executar essa verificação, o Security Hub primeiro usa a lógica personalizada para procurar o bucket do S3 em que seus CloudTrail registros estão armazenados. Em seguida, ele usa as regras AWS Config gerenciadas para verificar se o bucket está acessível ao público.

Se você agregar seus registros em um único bucket do S3 centralizado, o Security Hub executará a verificação somente na conta e na região em que o bucket do S3 centralizado está localizado. Para outras contas e regiões, o status do controle é Sem dados.

Se o bucket for descoberto e for acessível ao público, a verificação gerará uma descoberta com falha.

Correção

Para bloquear o acesso público ao seu bucket do CloudTrail S3, consulte Como definir configurações de bloqueio de acesso público para seus buckets do S3 no Guia do usuário do Amazon Simple Storage Service. O Bloqueio de acesso público do Amazon S3 fornece quatro configurações.

[CloudTrail.7] Certifique-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrail S3

Requisitos relacionados: CIS Foundations Benchmark v1.2.0/2.6, CIS AWS Foundations Benchmark v1.4.0/3.6, CIS AWS Foundations Benchmark v3.0.0/3.4 AWS

Categoria: Identificar > Registro em log

Severidade: baixa

Tipo de recurso

AWS Config regra: Nenhuma (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

O registro de acesso ao bucket do gera um log que contém os registros de acesso para cada solicitação feita no bucket do S3. Um registro contém detalhes sobre a solicitação, tais como o tipo da solicitação, os recursos especificados na solicitação e a data e hora em que a solicitação foi processada.

O CIS recomenda que você habilite o registro de acesso ao bucket no bucket do CloudTrail S3.

Ao habilitar o registro em log do bucket do S3 em buckets do S3 de destino, é possível capturar todos os eventos que podem afetar objetos em um bucket de destino. Configurar os logs para serem colocados em um bucket separado permite o acesso às informações de log, o que pode ser útil em fluxos de resposta a incidentes e segurança.

Para executar essa verificação, o Security Hub primeiro usa a lógica personalizada para procurar o bucket em que seus CloudTrail registros estão armazenados e, em seguida, usa a regra AWS Config gerenciada para verificar se o registro está ativado.

Se CloudTrail entregar arquivos de log de vários Contas da AWS em um único bucket Amazon S3 de destino, o Security Hub avalia esse controle somente em relação ao bucket de destino na região em que ele está localizado. Isso simplifica suas descobertas. No entanto, você deve ativar CloudTrail todas as contas que entregam registros ao bucket de destino. Para todas as contas, exceto aquela que contém o bucket de destino, o status do controle é Sem dados.

Se o bucket for descoberto e for acessível ao público, a verificação gerará uma descoberta com falha.

Correção

Para habilitar o registro de acesso ao servidor para seu bucket do CloudTrail S3, consulte Habilitar o registro de acesso ao servidor Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

[CloudTrail.9] CloudTrail trilhas devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-cloudtrail-trail` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	entre maiúsculas e minúsculas.			

Esse controle verifica se uma AWS CloudTrail trilha tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a trilha não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a trilha não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma CloudTrail trilha, consulte AddTagsna Referência da AWS CloudTrail API.

CloudWatch Controles da Amazon

Esses controles estão relacionados aos CloudWatch recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[CloudWatch.1] Um filtro métrico de log e um alarme devem existir para uso do usuário “root”

Requisitos relacionados: PCI DSS v3.2.1/7.2.1, CIS Foundations Benchmark v1.2.0/1.1, CIS Foundations Benchmark v1.2.0/3.3, CIS AWS Foundations Benchmark v1.4.0/1.7, CIS AWS Foundations Benchmark v1.4.0/4.3 AWS AWS

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso

AWS Config regra: Nenhuma (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

O usuário raiz tem acesso a todos os serviços e recursos da Conta da AWS na conta. É altamente recomendável que você evite usar o usuário raiz para tarefas diárias. Minimizar o uso dessa conta e adotar o princípio do privilégio mínimo para gerenciamento de acesso reduz o risco de alterações acidentais e divulgação não intencional de credenciais altamente privilegiadas.

Como uma melhor prática, use as credenciais raiz somente quando necessário para realizar tarefas de gerenciamento de serviços e da conta. Aplique políticas AWS Identity and Access Management (IAM) diretamente aos grupos e funções, mas não aos usuários. Para obter um tutorial sobre como configurar um administrador para uso diário, consulte Criar seu primeiro usuário administrador de IAM e grupo do no Guia do usuário do IAM

Para executar essa verificação, o Security Hub usa lógica personalizada para executar as etapas exatas de auditoria prescritas para o controle 1.7 no CIS AWS Foundations Benchmark v1.4.0. Haverá falha nesse controle se os filtros de métrica exatos prescritos pelo CIS não forem usados. Não é possível adicionar campos ou termos adicionais aos filtros de métrica.

Note

Quando o Security Hub executa a verificação desse controle, ele procura as CloudTrail trilhas que a conta atual usa. Essas trilhas podem ser trilhas da organização que pertencem a outra conta. As trilhas multirregionais também podem ser baseadas em uma região diferente.
A verificação resulta em descobertas `FAILED` nos seguintes casos:

- Nenhuma trilha está configurada.
- As trilhas disponíveis que estão na região atual e que são de propriedade da conta atual não atendem aos requisitos de controle.

A verificação resulta em um status de controle de `NO_DATA` nos seguintes casos:

- As trilhas multirregionais também podem ser baseadas em uma região diferente. O Security Hub só pode gerar descobertas na região em que a trilha está baseada.
- Uma trilha multirregional pertence a uma conta diferente. O Security Hub só pode gerar descobertas para a conta proprietária da trilha.

  Recomendamos trilhas organizacionais para registrar eventos de logs de várias contas em uma organização. Por padrão, as trilhas da organização são trilhas multirregionais e só podem ser gerenciadas pela conta AWS Organizations de gerenciamento ou pela conta de administrador CloudTrail delegado. O uso de uma trilha organizacional resulta em um status de controle de `NO_DATA` aos controles avaliados nas contas dos membros da organização. Nas contas dos membros, o Security Hub só gera descobertas para recursos de propriedade dos membros. As descobertas relacionadas às trilhas da organização são geradas na conta do proprietário do recurso. É possível ver essas descobertas em sua conta de administrador delegado do Security Hub usando a agregação entre regiões.

Para o alarme, a conta atual deve ser proprietária do tópico do Amazon SNS referenciado ou deve ter acesso ao tópico do Amazon SNS chamando `ListSubscriptionsByTopic`. Caso contrário, o Security Hub gera descobertas de `WARNING` para o controle.

Correção

Para passar por esse controle, siga estas etapas para criar um tópico do Amazon SNS, uma trilha de AWS CloudTrail , um filtro métrico e um alarme para o filtro métrico.

1. Criar um tópico do Amazon SNS. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service. Crie um tópico que receba todos os alarmes do CIS e crie pelo menos uma assinatura para o tópico.
2. Crie uma CloudTrail trilha que se aplique a todos Regiões da AWS. Para obter instruções, consulte Criação de um bucket no Guia do usuário do AWS CloudTrail (S3).

   Anote o nome do grupo de CloudWatch registros de registros que você associa à CloudTrail trilha. Você cria o filtro métrico para esse grupo de logs na próxima etapa.
3. Crie um filtro de métrica. Para obter instruções, consulte Criar um filtro métrico para um grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Definir padrão, padrão de filtro	`{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}`
namespace de métrica	**`LogMetrics`**
Valor da métrica	**`1`**
Valor padrão	**`0`**

4. Criar um alarme com base no filtro Para obter instruções, consulte Criação de um CloudWatch alarme com base em um filtro métrico de grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Condições, tipo de limite	Estático
Sempre que *`your-metric-name`* for...	Maior/Igual
THAN	**`1`**

[CloudWatch.2] Certifique-se de que exista um filtro métrico de registro e um alarme para chamadas de API não autorizadas

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.1

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso

AWS Config regra: Nenhuma (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode monitorar em tempo real as chamadas de API direcionando CloudTrail os registros para o CloudWatch Logs e estabelecendo filtros métricos e alarmes correspondentes.

Recomendamos que você crie um filtro e um alarme de métrica para chamadas de API não autorizadas. O monitoramento de chamadas de API não autorizadas ajuda a revelar erros de aplicativo e pode reduzir o tempo para detectar atividades mal-intencionadas.

Para executar essa verificação, o Security Hub usa lógica personalizada para executar as etapas exatas de auditoria prescritas para o controle 3.1 no CIS AWS Foundations Benchmark v1.2. Haverá falha nesse controle se os filtros de métrica exatos prescritos pelo CIS não forem usados. Não é possível adicionar campos ou termos adicionais aos filtros de métrica.

> **Note**
>
> Quando o Security Hub executa a verificação desse controle, ele procura as CloudTrail trilhas que a conta atual usa. Essas trilhas podem ser trilhas da organização que pertencem a outra conta. As trilhas multirregionais também podem ser baseadas em uma região diferente.
> A verificação resulta em descobertas `FAILED` nos seguintes casos:
>
> - Nenhuma trilha está configurada.
> - As trilhas disponíveis que estão na região atual e que são de propriedade da conta atual não atendem aos requisitos de controle.
>
> A verificação resulta em um status de controle de `NO_DATA` nos seguintes casos:

- As trilhas multirregionais também podem ser baseadas em uma região diferente. O Security Hub só pode gerar descobertas na região em que a trilha está baseada.
- Uma trilha multirregional pertence a uma conta diferente. O Security Hub só pode gerar descobertas para a conta proprietária da trilha.

  Recomendamos trilhas organizacionais para registrar eventos de logs de várias contas em uma organização. Por padrão, as trilhas da organização são trilhas multirregionais e só podem ser gerenciadas pela conta AWS Organizations de gerenciamento ou pela conta de administrador CloudTrail delegado. O uso de uma trilha organizacional resulta em um status de controle de `NO_DATA` aos controles avaliados nas contas dos membros da organização. Nas contas dos membros, o Security Hub só gera descobertas para recursos de propriedade dos membros. As descobertas relacionadas às trilhas da organização são geradas na conta do proprietário do recurso. É possível ver essas descobertas em sua conta de administrador delegado do Security Hub usando a agregação entre regiões.

Para o alarme, a conta atual deve ser proprietária do tópico do Amazon SNS referenciado ou deve ter acesso ao tópico do Amazon SNS chamando `ListSubscriptionsByTopic`. Caso contrário, o Security Hub gera descobertas de `WARNING` para o controle.

Correção

Para passar por esse controle, siga estas etapas para criar um tópico do Amazon SNS, uma trilha de AWS CloudTrail , um filtro métrico e um alarme para o filtro métrico.

1. Criar um tópico do Amazon SNS. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service. Crie um tópico que receba todos os alarmes do CIS e crie pelo menos uma assinatura para o tópico.
2. Crie uma CloudTrail trilha que se aplique a todos Regiões da AWS. Para obter instruções, consulte Criação de um bucket no Guia do usuário do AWS CloudTrail (S3).

   Anote o nome do grupo de CloudWatch registros de registros que você associa à CloudTrail trilha. Você cria o filtro métrico para esse grupo de logs na próxima etapa.
3. Crie um filtro de métrica. Para obter instruções, consulte Criar um filtro métrico para um grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Definir padrão, padrão de filtro	`{($.errorCode="*UnauthorizedOperation") \|\| ($.errorCode="AccessDenied*")}`
namespace de métrica	**`LogMetrics`**
Valor da métrica	**`1`**
Valor padrão	**`0`**

4. Criar um alarme com base no filtro Para obter instruções, consulte Criação de um CloudWatch alarme com base em um filtro métrico de grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Condições, tipo de limite	Estático
Sempre que *`your-metric-name`* for...	Maior/Igual
THAN	**`1`**

[CloudWatch.3] Certifique-se de que exista um filtro métrico de registro e um alarme para o login do Management Console sem MFA

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.2

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso

AWS Config regra: Nenhuma (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode monitorar em tempo real as chamadas de API direcionando CloudTrail os registros para o CloudWatch Logs e estabelecendo filtros métricos e alarmes correspondentes.

Recomendamos que você crie um filtro e um alarme de métrica para logins de console que não são protegidos por MFA. O monitoramento de logins de console com fator único aumenta a visibilidade em contas que não são protegidas por MFA.

Para executar essa verificação, o Security Hub usa lógica personalizada para executar as etapas exatas de auditoria prescritas para o controle 3.2 no CIS AWS Foundations Benchmark v1.2. Haverá falha nesse controle se os filtros de métrica exatos prescritos pelo CIS não forem usados. Não é possível adicionar campos ou termos adicionais aos filtros de métrica.

> **Note**
>
> Quando o Security Hub executa a verificação desse controle, ele procura as CloudTrail trilhas que a conta atual usa. Essas trilhas podem ser trilhas da organização que pertencem a outra conta. As trilhas multirregionais também podem ser baseadas em uma região diferente.
> A verificação resulta em descobertas `FAILED` nos seguintes casos:
>
> - Nenhuma trilha está configurada.
> - As trilhas disponíveis que estão na região atual e que são de propriedade da conta atual não atendem aos requisitos de controle.
>
> A verificação resulta em um status de controle de `NO_DATA` nos seguintes casos:
>
> - As trilhas multirregionais também podem ser baseadas em uma região diferente. O Security Hub só pode gerar descobertas na região em que a trilha está baseada.
> - Uma trilha multirregional pertence a uma conta diferente. O Security Hub só pode gerar descobertas para a conta proprietária da trilha.
>
>   Recomendamos trilhas organizacionais para registrar eventos de logs de várias contas em uma organização. Por padrão, as trilhas da organização são trilhas multirregionais e só podem ser gerenciadas pela conta AWS Organizations de gerenciamento ou pela conta de administrador CloudTrail delegado. O uso de uma trilha organizacional resulta em um status de controle de `NO_DATA` aos controles avaliados nas contas dos membros da organização. Nas contas dos membros, o Security Hub só gera descobertas para recursos de propriedade dos membros. As descobertas relacionadas às trilhas da organização são

geradas na conta do proprietário do recurso. É possível ver essas descobertas em sua conta de administrador delegado do Security Hub usando a agregação entre regiões.

Para o alarme, a conta atual deve ser proprietária do tópico do Amazon SNS referenciado ou deve ter acesso ao tópico do Amazon SNS chamando `ListSubscriptionsByTopic`. Caso contrário, o Security Hub gera descobertas de `WARNING` para o controle.

Correção

Para passar por esse controle, siga estas etapas para criar um tópico do Amazon SNS, uma trilha de AWS CloudTrail , um filtro métrico e um alarme para o filtro métrico.

1. Criar um tópico do Amazon SNS. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service. Crie um tópico que receba todos os alarmes do CIS e crie pelo menos uma assinatura para o tópico.
2. Crie uma CloudTrail trilha que se aplique a todos Regiões da AWS. Para obter instruções, consulte Criação de um bucket no Guia do usuário do AWS CloudTrail (S3).

   Anote o nome do grupo de CloudWatch registros de registros que você associa à CloudTrail trilha. Você cria o filtro métrico para esse grupo de logs na próxima etapa.
3. Crie um filtro de métrica. Para obter instruções, consulte Criar um filtro métrico para um grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Definir padrão, padrão de filtro	`{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes") && ($.userIdentity.type = "IAMUser") && ($.responseElements.ConsoleLogin = "Success") }`
namespace de métrica	**`LogMetrics`**
Valor da métrica	**`1`**

Campo	Valor
Valor padrão	**0**

4. Criar um alarme com base no filtro Para obter instruções, consulte Criação de um CloudWatch alarme com base em um filtro métrico de grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Condições, tipo de limite	Estático
Sempre que *your-metric-name* for...	Maior/Igual
THAN	**1**

[CloudWatch.4] Certifique-se de que exista um filtro de métrica de log e um alarme para alterações na política do IAM

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.4, CIS Foundations Benchmark v1.4.0/4.4 AWS

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso

AWS Config regra: Nenhuma (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se você monitora as chamadas de API em tempo real direcionando CloudTrail os CloudWatch registros para o Logs e estabelecendo filtros métricos e alarmes correspondentes.

Recomendamos que você crie um filtro de métrica e um alarme para fazer alterações em políticas do . Monitorar essas alterações ajuda a garantir que os controles de autenticação e autorização permaneçam intactos.

Note

Quando o Security Hub executa a verificação desse controle, ele procura as CloudTrail trilhas que a conta atual usa. Essas trilhas podem ser trilhas da organização que pertencem a outra conta. As trilhas multirregionais também podem ser baseadas em uma região diferente.
A verificação resulta em descobertas `FAILED` nos seguintes casos:

- Nenhuma trilha está configurada.
- As trilhas disponíveis que estão na região atual e que são de propriedade da conta atual não atendem aos requisitos de controle.

A verificação resulta em um status de controle de `NO_DATA` nos seguintes casos:

- As trilhas multirregionais também podem ser baseadas em uma região diferente. O Security Hub só pode gerar descobertas na região em que a trilha está baseada.
- Uma trilha multirregional pertence a uma conta diferente. O Security Hub só pode gerar descobertas para a conta proprietária da trilha.

  Recomendamos trilhas organizacionais para registrar eventos de logs de várias contas em uma organização. Por padrão, as trilhas da organização são trilhas multirregionais e só podem ser gerenciadas pela conta AWS Organizations de gerenciamento ou pela conta de administrador CloudTrail delegado. O uso de uma trilha organizacional resulta em um status de controle de `NO_DATA` aos controles avaliados nas contas dos membros da organização. Nas contas dos membros, o Security Hub só gera descobertas para recursos de propriedade dos membros. As descobertas relacionadas às trilhas da organização são geradas na conta do proprietário do recurso. É possível ver essas descobertas em sua conta de administrador delegado do Security Hub usando a agregação entre regiões.

Para o alarme, a conta atual deve ser proprietária do tópico do Amazon SNS referenciado ou deve ter acesso ao tópico do Amazon SNS chamando `ListSubscriptionsByTopic`. Caso contrário, o Security Hub gera descobertas de `WARNING` para o controle.

Correção

> **Note**
>
> Nosso padrão de filtro recomendado nessas etapas de correção difere do padrão de filtro na orientação do CIS. Nossos filtros recomendados têm como alvo somente eventos provenientes de chamadas de API do IAM.

Para passar por esse controle, siga estas etapas para criar um tópico do Amazon SNS, uma trilha de AWS CloudTrail , um filtro métrico e um alarme para o filtro métrico.

1. Criar um tópico do Amazon SNS. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service. Crie um tópico que receba todos os alarmes do CIS e crie pelo menos uma assinatura para o tópico.
2. Crie uma CloudTrail trilha que se aplique a todos Regiões da AWS. Para obter instruções, consulte Criação de um bucket no Guia do usuário do AWS CloudTrail (S3).

   Anote o nome do grupo de CloudWatch registros de registros que você associa à CloudTrail trilha. Você cria o filtro métrico para esse grupo de logs na próxima etapa.
3. Crie um filtro de métrica. Para obter instruções, consulte Criar um filtro métrico para um grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Definir padrão, padrão de filtro	`{($.eventSource=iam.amazonaws.com) && (($.eventName=DeleteGroupPolicy) || ($.eventName=DeleteRolePolicy) \|\| ($.eventName=DeleteUserPolicy) || ($.eventName=PutGroupPolicy) \|\| ($.eventName=PutRolePolicy) || ($.eventName=PutUserPolicy) \|\| ($.eventName=CreatePolicy) || ($.eventName=DeletePolicy) \|\| ($.eventName=CreatePolicyVersion) || ($.eventN`

Campo	Valor
	`ame=DeletePolicyVersion) || ($.eventName=AttachRolePoli cy) \|\| ($.eventName=Detac hRolePolicy) || ($.eventN ame=AttachUserPolicy) \|\| ($.eventName=DetachUserPolicy) || ($.eventName=AttachGroupPol icy) \|\| ($.eventName=Detac hGroupPolicy))}`
namespace de métrica	**`LogMetrics`**
Valor da métrica	**`1`**
Valor padrão	**`0`**

4. Criar um alarme com base no filtro Para obter instruções, consulte Criação de um CloudWatch alarme com base em um filtro métrico de grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Condições, tipo de limite	Estático
Sempre que *`your-metric-name`* for...	Maior/Igual
THAN	**`1`**

[CloudWatch.5] Certifique-se de que exista um filtro métrico de log e um alarme para alterações de CloudTrail AWS Config duração

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.5, CIS Foundations Benchmark v1.4.0/4.5 AWS

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso

AWS Config regra: Nenhuma (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode monitorar em tempo real as chamadas de API direcionando CloudTrail os registros para o CloudWatch Logs e estabelecendo filtros métricos e alarmes correspondentes.

O CIS recomenda que você crie um filtro métrico e um alarme para alterações nas CloudTrail configurações. Monitorar essas alterações ajuda a garantir visibilidade sustentada para atividades na conta.

Para executar essa verificação, o Security Hub usa lógica personalizada para executar as etapas exatas de auditoria prescritas para o controle 4.5 no CIS AWS Foundations Benchmark v1.4.0. Haverá falha nesse controle se os filtros de métrica exatos prescritos pelo CIS não forem usados. Não é possível adicionar campos ou termos adicionais aos filtros de métrica.

> **Note**
>
> Quando o Security Hub executa a verificação desse controle, ele procura as CloudTrail trilhas que a conta atual usa. Essas trilhas podem ser trilhas da organização que pertencem a outra conta. As trilhas multirregionais também podem ser baseadas em uma região diferente.
> A verificação resulta em descobertas `FAILED` nos seguintes casos:
>
> - Nenhuma trilha está configurada.
> - As trilhas disponíveis que estão na região atual e que são de propriedade da conta atual não atendem aos requisitos de controle.
>
> A verificação resulta em um status de controle de `NO_DATA` nos seguintes casos:
>
> - As trilhas multirregionais também podem ser baseadas em uma região diferente. O Security Hub só pode gerar descobertas na região em que a trilha está baseada.
> - Uma trilha multirregional pertence a uma conta diferente. O Security Hub só pode gerar descobertas para a conta proprietária da trilha.
>
>   Recomendamos trilhas organizacionais para registrar eventos de logs de várias contas em uma organização. Por padrão, as trilhas da organização são trilhas multirregionais

e só podem ser gerenciadas pela conta AWS Organizations de gerenciamento ou pela conta de administrador CloudTrail delegado. O uso de uma trilha organizacional resulta em um status de controle de `NO_DATA` aos controles avaliados nas contas dos membros da organização. Nas contas dos membros, o Security Hub só gera descobertas para recursos de propriedade dos membros. As descobertas relacionadas às trilhas da organização são geradas na conta do proprietário do recurso. É possível ver essas descobertas em sua conta de administrador delegado do Security Hub usando a agregação entre regiões.

Para o alarme, a conta atual deve ser proprietária do tópico do Amazon SNS referenciado ou deve ter acesso ao tópico do Amazon SNS chamando `ListSubscriptionsByTopic`. Caso contrário, o Security Hub gera descobertas de `WARNING` para o controle.

Correção

Para passar por esse controle, siga estas etapas para criar um tópico do Amazon SNS, uma trilha de AWS CloudTrail , um filtro métrico e um alarme para o filtro métrico.

1. Criar um tópico do Amazon SNS. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service. Crie um tópico que receba todos os alarmes do CIS e crie pelo menos uma assinatura para o tópico.
2. Crie uma CloudTrail trilha que se aplique a todos Regiões da AWS. Para obter instruções, consulte Criação de um bucket no Guia do usuário do AWS CloudTrail (S3).

   Anote o nome do grupo de CloudWatch registros de registros que você associa à CloudTrail trilha. Você cria o filtro métrico para esse grupo de logs na próxima etapa.
3. Crie um filtro de métrica. Para obter instruções, consulte Criar um filtro métrico para um grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Definir padrão, padrão de filtro	`{($.eventName=CreateTrail) \|\| ($.eventName=UpdateTrail) || ($.eventName=DeleteTrail) \|\| ($.eventName=StartLogging) || ($.eventName=StopLogging)}`

Campo	Valor
namespace de métrica	**`LogMetrics`**
Valor da métrica	**`1`**
Valor padrão	**`0`**

4. Criar um alarme com base no filtro Para obter instruções, consulte Criação de um CloudWatch alarme com base em um filtro métrico de grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Condições, tipo de limite	Estático
Sempre que *`your-metric-name`* for...	Maior/Igual
THAN	**`1`**

[CloudWatch.6] Certifique-se de que exista um filtro métrico de registro e um alarme para falhas de AWS Management Console autenticação

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.6, CIS Foundations Benchmark v1.4.0/4.6 AWS

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso

AWS Config regra: Nenhuma (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode monitorar em tempo real as chamadas de API direcionando CloudTrail os registros para o CloudWatch Logs e estabelecendo filtros métricos e alarmes correspondentes.

Recomendamos que você crie um filtro e um alarme de métrica para tentativas com falha de autenticação no console. O monitoramento de logins de console com falha pode diminuir o tempo necessário para detectar uma tentativa de inserção forçada de uma credencial, o que pode fornecer um indicador, como o IP de origem, que pode ser usado em outras correlações do evento.

Para executar essa verificação, o Security Hub usa lógica personalizada para executar as etapas exatas de auditoria prescritas para o controle 4.6 no CIS AWS Foundations Benchmark v1.4.0. Haverá falha nesse controle se os filtros de métrica exatos prescritos pelo CIS não forem usados. Não é possível adicionar campos ou termos adicionais aos filtros de métrica.

Note

Quando o Security Hub executa a verificação desse controle, ele procura as CloudTrail trilhas que a conta atual usa. Essas trilhas podem ser trilhas da organização que pertencem a outra conta. As trilhas multirregionais também podem ser baseadas em uma região diferente.
A verificação resulta em descobertas `FAILED` nos seguintes casos:

- Nenhuma trilha está configurada.
- As trilhas disponíveis que estão na região atual e que são de propriedade da conta atual não atendem aos requisitos de controle.

A verificação resulta em um status de controle de `NO_DATA` nos seguintes casos:

- As trilhas multirregionais também podem ser baseadas em uma região diferente. O Security Hub só pode gerar descobertas na região em que a trilha está baseada.
- Uma trilha multirregional pertence a uma conta diferente. O Security Hub só pode gerar descobertas para a conta proprietária da trilha.

  Recomendamos trilhas organizacionais para registrar eventos de logs de várias contas em uma organização. Por padrão, as trilhas da organização são trilhas multirregionais e só podem ser gerenciadas pela conta AWS Organizations de gerenciamento ou pela conta de administrador CloudTrail delegado. O uso de uma trilha organizacional resulta em um status de controle de `NO_DATA` aos controles avaliados nas contas dos membros da organização. Nas contas dos membros, o Security Hub só gera descobertas para recursos de propriedade dos membros. As descobertas relacionadas às trilhas da organização são geradas na conta do proprietário do recurso. É possível ver essas descobertas em sua conta de administrador delegado do Security Hub usando a agregação entre regiões.

Para o alarme, a conta atual deve ser proprietária do tópico do Amazon SNS referenciado ou deve ter acesso ao tópico do Amazon SNS chamando `ListSubscriptionsByTopic`. Caso contrário, o Security Hub gera descobertas de `WARNING` para o controle.

Correção

Para passar por esse controle, siga estas etapas para criar um tópico do Amazon SNS, uma trilha de AWS CloudTrail , um filtro métrico e um alarme para o filtro métrico.

1. Criar um tópico do Amazon SNS. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service. Crie um tópico que receba todos os alarmes do CIS e crie pelo menos uma assinatura para o tópico.
2. Crie uma CloudTrail trilha que se aplique a todos Regiões da AWS. Para obter instruções, consulte Criação de um bucket no Guia do usuário do AWS CloudTrail (S3).

   Anote o nome do grupo de CloudWatch registros de registros que você associa à CloudTrail trilha. Você cria o filtro métrico para esse grupo de logs na próxima etapa.
3. Crie um filtro de métrica. Para obter instruções, consulte Criar um filtro métrico para um grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Definir padrão, padrão de filtro	`{($.eventName=ConsoleLogin) && ($.errorMessage="Failed authentication")}`
namespace de métrica	**`LogMetrics`**
Valor da métrica	**`1`**
Valor padrão	**`0`**

4. Criar um alarme com base no filtro Para obter instruções, consulte Criação de um CloudWatch alarme com base em um filtro métrico de grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Condições, tipo de limite	Estático
Sempre que *your-metric-name* for...	Maior/Igual
THAN	**1**

[CloudWatch.7] Certifique-se de que exista um filtro métrico de registro e um alarme para desativar ou excluir programadamente as chaves gerenciadas pelo cliente

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.7, CIS Foundations Benchmark v1.4.0/4.7 AWS

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso

AWS Config regra: Nenhuma (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode monitorar em tempo real as chamadas de API direcionando CloudTrail os registros para o CloudWatch Logs e estabelecendo filtros métricos e alarmes correspondentes.

Recomendamos que você crie um filtro e um alarme de métrica para CMKs criadas pelo cliente cujo estado foi alterado para desativado ou exclusão programada. Os dados criptografados com chaves desativadas ou excluídas não podem mais ser acessados.

Para executar essa verificação, o Security Hub usa lógica personalizada para executar as etapas de auditoria exatas prescritas para o controle 4.7 no CIS AWS Foundations Benchmark v1.4.0. Haverá falha nesse controle se os filtros de métrica exatos prescritos pelo CIS não forem usados. Não é possível adicionar campos ou termos adicionais aos filtros de métrica. O controle também falhará se `ExcludeManagementEventSources` contiver `kms.amazonaws.com`.

Note

Quando o Security Hub executa a verificação desse controle, ele procura as CloudTrail trilhas que a conta atual usa. Essas trilhas podem ser trilhas da organização que pertencem a outra conta. As trilhas multirregionais também podem ser baseadas em uma região diferente.
A verificação resulta em descobertas `FAILED` nos seguintes casos:

- Nenhuma trilha está configurada.
- As trilhas disponíveis que estão na região atual e que são de propriedade da conta atual não atendem aos requisitos de controle.

A verificação resulta em um status de controle de `NO_DATA` nos seguintes casos:

- As trilhas multirregionais também podem ser baseadas em uma região diferente. O Security Hub só pode gerar descobertas na região em que a trilha está baseada.
- Uma trilha multirregional pertence a uma conta diferente. O Security Hub só pode gerar descobertas para a conta proprietária da trilha.

  Recomendamos trilhas organizacionais para registrar eventos de logs de várias contas em uma organização. Por padrão, as trilhas da organização são trilhas multirregionais e só podem ser gerenciadas pela conta AWS Organizations de gerenciamento ou pela conta de administrador CloudTrail delegado. O uso de uma trilha organizacional resulta em um status de controle de `NO_DATA` aos controles avaliados nas contas dos membros da organização. Nas contas dos membros, o Security Hub só gera descobertas para recursos de propriedade dos membros. As descobertas relacionadas às trilhas da organização são geradas na conta do proprietário do recurso. É possível ver essas descobertas em sua conta de administrador delegado do Security Hub usando a agregação entre regiões.

Para o alarme, a conta atual deve ser proprietária do tópico do Amazon SNS referenciado ou deve ter acesso ao tópico do Amazon SNS chamando `ListSubscriptionsByTopic`. Caso contrário, o Security Hub gera descobertas de `WARNING` para o controle.

Correção

Para passar por esse controle, siga estas etapas para criar um tópico do Amazon SNS, uma trilha de AWS CloudTrail , um filtro métrico e um alarme para o filtro métrico.

1. Criar um tópico do Amazon SNS. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service. Crie um tópico que receba todos os alarmes do CIS e crie pelo menos uma assinatura para o tópico.
2. Crie uma CloudTrail trilha que se aplique a todos Regiões da AWS. Para obter instruções, consulte Criação de um bucket no Guia do usuário do AWS CloudTrail (S3).

   Anote o nome do grupo de CloudWatch registros de registros que você associa à CloudTrail trilha. Você cria o filtro métrico para esse grupo de logs na próxima etapa.
3. Crie um filtro de métrica. Para obter instruções, consulte Criar um filtro métrico para um grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Definir padrão, padrão de filtro	`{($.eventSource=kms.amazonaws.com) && (($.eventName=DisableKey) || ($.eventName=ScheduleKeyDeletion))}`
namespace de métrica	**`LogMetrics`**
Valor da métrica	**`1`**
Valor padrão	**`0`**

4. Criar um alarme com base no filtro Para obter instruções, consulte Criação de um CloudWatch alarme com base em um filtro métrico de grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Condições, tipo de limite	Estático
Sempre que *`your-metric-name`* for...	Maior/Igual
THAN	**`1`**

[CloudWatch.8] Certifique-se de que exista um filtro métrico de log e um alarme para alterações na política do bucket do S3

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.8, CIS Foundations Benchmark v1.4.0/4.8 AWS

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso

AWS Config regra: Nenhuma (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode monitorar em tempo real as chamadas de API direcionando CloudTrail os registros para o CloudWatch Logs e estabelecendo filtros métricos e alarmes correspondentes.

Recomendamos que você crie um filtro de métrica e um alarme para fazer alterações em políticas de bucket do S3. Monitorar essas alterações pode reduzir o tempo para detectar e corrigir políticas permissivas em buckets do S3 confidenciais.

Para executar essa verificação, o Security Hub usa lógica personalizada para executar as etapas de auditoria exatas prescritas para o controle 4.8 no CIS AWS Foundations Benchmark v1.4.0. Haverá falha nesse controle se os filtros de métrica exatos prescritos pelo CIS não forem usados. Não é possível adicionar campos ou termos adicionais aos filtros de métrica.

> **Note**
>
> Quando o Security Hub executa a verificação desse controle, ele procura as CloudTrail trilhas que a conta atual usa. Essas trilhas podem ser trilhas da organização que pertencem a outra conta. As trilhas multirregionais também podem ser baseadas em uma região diferente.
> A verificação resulta em descobertas `FAILED` nos seguintes casos:
>
> - Nenhuma trilha está configurada.
> - As trilhas disponíveis que estão na região atual e que são de propriedade da conta atual não atendem aos requisitos de controle.

A verificação resulta em um status de controle de `NO_DATA` nos seguintes casos:

- As trilhas multirregionais também podem ser baseadas em uma região diferente. O Security Hub só pode gerar descobertas na região em que a trilha está baseada.
- Uma trilha multirregional pertence a uma conta diferente. O Security Hub só pode gerar descobertas para a conta proprietária da trilha.

  Recomendamos trilhas organizacionais para registrar eventos de logs de várias contas em uma organização. Por padrão, as trilhas da organização são trilhas multirregionais e só podem ser gerenciadas pela conta AWS Organizations de gerenciamento ou pela conta de administrador CloudTrail delegado. O uso de uma trilha organizacional resulta em um status de controle de `NO_DATA` aos controles avaliados nas contas dos membros da organização. Nas contas dos membros, o Security Hub só gera descobertas para recursos de propriedade dos membros. As descobertas relacionadas às trilhas da organização são geradas na conta do proprietário do recurso. É possível ver essas descobertas em sua conta de administrador delegado do Security Hub usando a agregação entre regiões.

Para o alarme, a conta atual deve ser proprietária do tópico do Amazon SNS referenciado ou deve ter acesso ao tópico do Amazon SNS chamando `ListSubscriptionsByTopic`. Caso contrário, o Security Hub gera descobertas de `WARNING` para o controle.

Correção

Para passar por esse controle, siga estas etapas para criar um tópico do Amazon SNS, uma trilha de AWS CloudTrail , um filtro métrico e um alarme para o filtro métrico.

1. Criar um tópico do Amazon SNS. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service. Crie um tópico que receba todos os alarmes do CIS e crie pelo menos uma assinatura para o tópico.
2. Crie uma CloudTrail trilha que se aplique a todos Regiões da AWS. Para obter instruções, consulte Criação de um bucket no Guia do usuário do AWS CloudTrail (S3).

   Anote o nome do grupo de CloudWatch registros de registros que você associa à CloudTrail trilha. Você cria o filtro métrico para esse grupo de logs na próxima etapa.

3. Crie um filtro de métrica. Para obter instruções, consulte Criar um filtro métrico para um grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Definir padrão, padrão de filtro	`{($.eventSource=s3.amazonaws.com) && (($.eventName=PutBucketAcl) || ($.eventName=PutBucketPolicy) \|\| ($.eventName=PutBucketCors) || ($.eventName=PutBucketLifecycle) \|\| ($.eventName=PutBucketReplication) || ($.eventName=DeleteBucketPolicy) \|\| ($.eventName=DeleteBucketCors) || ($.eventName=DeleteBucketLifecycle) \|\| ($.eventName=DeleteBucketReplication))}`
namespace de métrica	**`LogMetrics`**
Valor da métrica	**`1`**
Valor padrão	**`0`**

4. Criar um alarme com base no filtro Para obter instruções, consulte Criação de um CloudWatch alarme com base em um filtro métrico de grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Condições, tipo de limite	Estático
Sempre que *`your-metric-name`* for...	Maior/Igual
THAN	**`1`**

[CloudWatch.9] Certifique-se de que exista um filtro métrico de registro e um alarme para alterações AWS Config de configuração

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.9, CIS Foundations Benchmark v1.4.0/4.9 AWS

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso

AWS Config regra: Nenhuma (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode monitorar em tempo real as chamadas de API direcionando CloudTrail os registros para o CloudWatch Logs e estabelecendo filtros métricos e alarmes correspondentes.

Recomendamos que você crie um filtro de métrica e um alarme para fazer alterações em opções de configuração do AWS Config . Monitorar essas alterações ajuda a garantir a visibilidade sustentada de itens de configuração na conta.

Para executar essa verificação, o Security Hub usa lógica personalizada para executar as etapas de auditoria exatas prescritas para o controle 4.9 no CIS AWS Foundations Benchmark v1.4.0. Haverá falha nesse controle se os filtros de métrica exatos prescritos pelo CIS não forem usados. Não é possível adicionar campos ou termos adicionais aos filtros de métrica.

> **Note**
>
> Quando o Security Hub executa a verificação desse controle, ele procura as CloudTrail trilhas que a conta atual usa. Essas trilhas podem ser trilhas da organização que pertencem a outra conta. As trilhas multirregionais também podem ser baseadas em uma região diferente.
> A verificação resulta em descobertas `FAILED` nos seguintes casos:
>
> - Nenhuma trilha está configurada.
> - As trilhas disponíveis que estão na região atual e que são de propriedade da conta atual não atendem aos requisitos de controle.

A verificação resulta em um status de controle de `NO_DATA` nos seguintes casos:

- As trilhas multirregionais também podem ser baseadas em uma região diferente. O Security Hub só pode gerar descobertas na região em que a trilha está baseada.
- Uma trilha multirregional pertence a uma conta diferente. O Security Hub só pode gerar descobertas para a conta proprietária da trilha.

  Recomendamos trilhas organizacionais para registrar eventos de logs de várias contas em uma organização. Por padrão, as trilhas da organização são trilhas multirregionais e só podem ser gerenciadas pela conta AWS Organizations de gerenciamento ou pela conta de administrador CloudTrail delegado. O uso de uma trilha organizacional resulta em um status de controle de `NO_DATA` aos controles avaliados nas contas dos membros da organização. Nas contas dos membros, o Security Hub só gera descobertas para recursos de propriedade dos membros. As descobertas relacionadas às trilhas da organização são geradas na conta do proprietário do recurso. É possível ver essas descobertas em sua conta de administrador delegado do Security Hub usando a agregação entre regiões.

Para o alarme, a conta atual deve ser proprietária do tópico do Amazon SNS referenciado ou deve ter acesso ao tópico do Amazon SNS chamando `ListSubscriptionsByTopic`. Caso contrário, o Security Hub gera descobertas de `WARNING` para o controle.

Correção

Para passar por esse controle, siga estas etapas para criar um tópico do Amazon SNS, uma trilha de AWS CloudTrail , um filtro métrico e um alarme para o filtro métrico.

1. Criar um tópico do Amazon SNS. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service. Crie um tópico que receba todos os alarmes do CIS e crie pelo menos uma assinatura para o tópico.
2. Crie uma CloudTrail trilha que se aplique a todos Regiões da AWS. Para obter instruções, consulte Criação de um bucket no Guia do usuário do AWS CloudTrail (S3).

   Anote o nome do grupo de CloudWatch registros de registros que você associa à CloudTrail trilha. Você cria o filtro métrico para esse grupo de logs na próxima etapa.

3. Crie um filtro de métrica. Para obter instruções, consulte Criar um filtro métrico para um grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Definir padrão, padrão de filtro	`{($.eventSource=config.amazonaws.com) && (($.eventName=StopConfigurationRecorder) || ($.eventName=DeleteDeliveryChannel) \|\| ($.eventName=PutDeliveryChannel) || ($.eventName=PutConfigurationRecorder))}`
namespace de métrica	**`LogMetrics`**
Valor da métrica	**`1`**
Valor padrão	**`0`**

4. Criar um alarme com base no filtro Para obter instruções, consulte Criação de um CloudWatch alarme com base em um filtro métrico de grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Condições, tipo de limite	Estático
Sempre que *`your-metric-name`* for...	Maior/Igual
THAN	**`1`**

[CloudWatch.10] Certifique-se de que exista um filtro métrico de log e um alarme para alterações no grupo de segurança

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.10, CIS Foundations Benchmark v1.4.0/4.10 AWS

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso

AWS Config regra: Nenhuma (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode monitorar em tempo real as chamadas de API direcionando CloudTrail os registros para o CloudWatch Logs e estabelecendo filtros métricos e alarmes correspondentes. Os grupos de segurança são um filtro de pacote com estado que controla o tráfego de entrada e saída em uma VPC.

Recomendamos que você crie um filtro de métrica e um alarme para fazer alterações em grupos de segurança. Monitorar essas alterações ajuda a garantir que os recursos e serviços da não sejam expostos involuntariamente.

Para executar essa verificação, o Security Hub usa lógica personalizada para executar as etapas exatas de auditoria prescritas para o controle 4.10 no CIS AWS Foundations Benchmark v1.4.0. Haverá falha nesse controle se os filtros de métrica exatos prescritos pelo CIS não forem usados. Não é possível adicionar campos ou termos adicionais aos filtros de métrica.

> **Note**
>
> Quando o Security Hub executa a verificação desse controle, ele procura as CloudTrail trilhas que a conta atual usa. Essas trilhas podem ser trilhas da organização que pertencem a outra conta. As trilhas multirregionais também podem ser baseadas em uma região diferente.
> A verificação resulta em descobertas `FAILED` nos seguintes casos:
>
> - Nenhuma trilha está configurada.
> - As trilhas disponíveis que estão na região atual e que são de propriedade da conta atual não atendem aos requisitos de controle.
>
> A verificação resulta em um status de controle de `NO_DATA` nos seguintes casos:
>
> - As trilhas multirregionais também podem ser baseadas em uma região diferente. O Security Hub só pode gerar descobertas na região em que a trilha está baseada.

- Uma trilha multirregional pertence a uma conta diferente. O Security Hub só pode gerar descobertas para a conta proprietária da trilha.

  Recomendamos trilhas organizacionais para registrar eventos de logs de várias contas em uma organização. Por padrão, as trilhas da organização são trilhas multirregionais e só podem ser gerenciadas pela conta AWS Organizations de gerenciamento ou pela conta de administrador CloudTrail delegado. O uso de uma trilha organizacional resulta em um status de controle de `NO_DATA` aos controles avaliados nas contas dos membros da organização. Nas contas dos membros, o Security Hub só gera descobertas para recursos de propriedade dos membros. As descobertas relacionadas às trilhas da organização são geradas na conta do proprietário do recurso. É possível ver essas descobertas em sua conta de administrador delegado do Security Hub usando a agregação entre regiões.

Para o alarme, a conta atual deve ser proprietária do tópico do Amazon SNS referenciado ou deve ter acesso ao tópico do Amazon SNS chamando `ListSubscriptionsByTopic`. Caso contrário, o Security Hub gera descobertas de `WARNING` para o controle.

Correção

Para passar por esse controle, siga estas etapas para criar um tópico do Amazon SNS, uma trilha de AWS CloudTrail , um filtro métrico e um alarme para o filtro métrico.

1. Criar um tópico do Amazon SNS. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service. Crie um tópico que receba todos os alarmes do CIS e crie pelo menos uma assinatura para o tópico.
2. Crie uma CloudTrail trilha que se aplique a todos Regiões da AWS. Para obter instruções, consulte Criação de um bucket no Guia do usuário do AWS CloudTrail (S3).

   Anote o nome do grupo de CloudWatch registros de registros que você associa à CloudTrail trilha. Você cria o filtro métrico para esse grupo de logs na próxima etapa.
3. Crie um filtro de métrica. Para obter instruções, consulte Criar um filtro métrico para um grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Definir padrão, padrão de filtro	`{($.eventName=AuthorizeSecurityGroupIngress) \|\| ($.eventName=AuthorizeSecurityGroupEgress) || ($.eventName=RevokeSecurityGroupIngress) \|\| ($.eventName=RevokeSecurityGroupEgress) || ($.eventName=CreateSecurityGroup) \|\| ($.eventName=DeleteSecurityGroup)}`
namespace de métrica	**`LogMetrics`**
Valor da métrica	**`1`**
Valor padrão	**`0`**

4. Criar um alarme com base no filtro Para obter instruções, consulte Criação de um CloudWatch alarme com base em um filtro métrico de grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Condições, tipo de limite	Estático
Sempre que *`your-metric-name`* for...	Maior/Igual
THAN	**`1`**

[CloudWatch.11] Certifique-se de que exista um filtro métrico de registro e um alarme para alterações nas listas de controle de acesso à rede (NACL)

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.11, CIS Foundations Benchmark v1.4.0/4.11 AWS

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso

AWS Config regra: Nenhuma (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode monitorar em tempo real as chamadas de API direcionando CloudTrail os registros para o CloudWatch Logs e estabelecendo filtros métricos e alarmes correspondentes. As NACLs são usadas como um filtro de pacote sem estado para controlar o tráfego de entrada e saída para sub-redes em uma VPC.

Recomendamos que você crie um filtro de métrica e um alarme para fazer alterações em NACLs. O monitoramento dessas mudanças ajuda a garantir que AWS recursos e serviços não sejam expostos acidentalmente.

Para executar essa verificação, o Security Hub usa lógica personalizada para executar as etapas exatas de auditoria prescritas para o controle 4.11 no CIS AWS Foundations Benchmark v1.4.0. Haverá falha nesse controle se os filtros de métrica exatos prescritos pelo CIS não forem usados. Não é possível adicionar campos ou termos adicionais aos filtros de métrica.

> **Note**
>
> Quando o Security Hub executa a verificação desse controle, ele procura as CloudTrail trilhas que a conta atual usa. Essas trilhas podem ser trilhas da organização que pertencem a outra conta. As trilhas multirregionais também podem ser baseadas em uma região diferente.
> A verificação resulta em descobertas `FAILED` nos seguintes casos:
>
> - Nenhuma trilha está configurada.
> - As trilhas disponíveis que estão na região atual e que são de propriedade da conta atual não atendem aos requisitos de controle.
>
> A verificação resulta em um status de controle de `NO_DATA` nos seguintes casos:
>
> - As trilhas multirregionais também podem ser baseadas em uma região diferente. O Security Hub só pode gerar descobertas na região em que a trilha está baseada.

- Uma trilha multirregional pertence a uma conta diferente. O Security Hub só pode gerar descobertas para a conta proprietária da trilha.

  Recomendamos trilhas organizacionais para registrar eventos de logs de várias contas em uma organização. Por padrão, as trilhas da organização são trilhas multirregionais e só podem ser gerenciadas pela conta AWS Organizations de gerenciamento ou pela conta de administrador CloudTrail delegado. O uso de uma trilha organizacional resulta em um status de controle de `NO_DATA` aos controles avaliados nas contas dos membros da organização. Nas contas dos membros, o Security Hub só gera descobertas para recursos de propriedade dos membros. As descobertas relacionadas às trilhas da organização são geradas na conta do proprietário do recurso. É possível ver essas descobertas em sua conta de administrador delegado do Security Hub usando a agregação entre regiões.

Para o alarme, a conta atual deve ser proprietária do tópico do Amazon SNS referenciado ou deve ter acesso ao tópico do Amazon SNS chamando `ListSubscriptionsByTopic`. Caso contrário, o Security Hub gera descobertas de `WARNING` para o controle.

Correção

Para passar por esse controle, siga estas etapas para criar um tópico do Amazon SNS, uma trilha de AWS CloudTrail , um filtro métrico e um alarme para o filtro métrico.

1. Criar um tópico do Amazon SNS. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service. Crie um tópico que receba todos os alarmes do CIS e crie pelo menos uma assinatura para o tópico.
2. Crie uma CloudTrail trilha que se aplique a todos Regiões da AWS. Para obter instruções, consulte Criação de um bucket no Guia do usuário do AWS CloudTrail (S3).

   Anote o nome do grupo de CloudWatch registros de registros que você associa à CloudTrail trilha. Você cria o filtro métrico para esse grupo de logs na próxima etapa.
3. Crie um filtro de métrica. Para obter instruções, consulte Criar um filtro métrico para um grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Definir padrão, padrão de filtro	`{($.eventName=CreateNetworkAcl) \|\| ($.eventName=CreateNetworkAclEntry) || ($.eventName=DeleteNetworkAcl) \|\| ($.eventName=DeleteNetworkAclEntry) || ($.eventName=ReplaceNetworkAclEntry) \|\| ($.eventName=ReplaceNetworkAclAssociation)}`
namespace de métrica	**`LogMetrics`**
Valor da métrica	**`1`**
Valor padrão	**`0`**

4. Criar um alarme com base no filtro Para obter instruções, consulte Criação de um CloudWatch alarme com base em um filtro métrico de grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Condições, tipo de limite	Estático
Sempre que *`your-metric-name`* for...	Maior/Igual
THAN	**`1`**

[CloudWatch.12] Certifique-se de que exista um filtro métrico de log e um alarme para alterações nos gateways de rede

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.12, CIS Foundations Benchmark v1.4.0/4.12 AWS

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso

AWS Config regra: Nenhuma (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode monitorar em tempo real as chamadas de API direcionando CloudTrail os registros para o CloudWatch Logs e estabelecendo filtros métricos e alarmes correspondentes. Os gateways de rede são necessários para enviar e receber tráfego para um destino fora de uma VPC.

Recomendamos que você crie um filtro de métrica e um alarme para fazer alterações em gateways de rede. Monitorar essas alterações ajuda a garantir que todo o tráfego de entrada e saída passará pela borda da VPC por um caminho controlado.

Para executar essa verificação, o Security Hub usa lógica personalizada para executar as etapas exatas de auditoria prescritas para o controle 4.12 no CIS AWS Foundations Benchmark v1.2. Haverá falha nesse controle se os filtros de métrica exatos prescritos pelo CIS não forem usados. Não é possível adicionar campos ou termos adicionais aos filtros de métrica.

> **Note**
>
> Quando o Security Hub executa a verificação desse controle, ele procura as CloudTrail trilhas que a conta atual usa. Essas trilhas podem ser trilhas da organização que pertencem a outra conta. As trilhas multirregionais também podem ser baseadas em uma região diferente.
> A verificação resulta em descobertas `FAILED` nos seguintes casos:
>
> - Nenhuma trilha está configurada.
> - As trilhas disponíveis que estão na região atual e que são de propriedade da conta atual não atendem aos requisitos de controle.
>
> A verificação resulta em um status de controle de `NO_DATA` nos seguintes casos:
>
> - As trilhas multirregionais também podem ser baseadas em uma região diferente. O Security Hub só pode gerar descobertas na região em que a trilha está baseada.
> - Uma trilha multirregional pertence a uma conta diferente. O Security Hub só pode gerar descobertas para a conta proprietária da trilha.

Recomendamos trilhas organizacionais para registrar eventos de logs de várias contas em uma organização. Por padrão, as trilhas da organização são trilhas multirregionais e só podem ser gerenciadas pela conta AWS Organizations de gerenciamento ou pela conta de administrador CloudTrail delegado. O uso de uma trilha organizacional resulta em um status de controle de `NO_DATA` aos controles avaliados nas contas dos membros da organização. Nas contas dos membros, o Security Hub só gera descobertas para recursos de propriedade dos membros. As descobertas relacionadas às trilhas da organização são geradas na conta do proprietário do recurso. É possível ver essas descobertas em sua conta de administrador delegado do Security Hub usando a agregação entre regiões.

Para o alarme, a conta atual deve ser proprietária do tópico do Amazon SNS referenciado ou deve ter acesso ao tópico do Amazon SNS chamando `ListSubscriptionsByTopic`. Caso contrário, o Security Hub gera descobertas de `WARNING` para o controle.

Correção

Para passar por esse controle, siga estas etapas para criar um tópico do Amazon SNS, uma trilha de AWS CloudTrail , um filtro métrico e um alarme para o filtro métrico.

1. Criar um tópico do Amazon SNS. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service. Crie um tópico que receba todos os alarmes do CIS e crie pelo menos uma assinatura para o tópico.
2. Crie uma CloudTrail trilha que se aplique a todos Regiões da AWS. Para obter instruções, consulte Criação de um bucket no Guia do usuário do AWS CloudTrail (S3).

   Anote o nome do grupo de CloudWatch registros de registros que você associa à CloudTrail trilha. Você cria o filtro métrico para esse grupo de logs na próxima etapa.
3. Crie um filtro de métrica. Para obter instruções, consulte Criar um filtro métrico para um grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Definir padrão, padrão de filtro	`{($.eventName=CreateCustomerGateway) \|\| ($.eventName=DeleteCustomerGateway) || ($.eventN`

Campo	Valor
	`ame=AttachInternetGateway) || ($.eventName=CreateInternet Gateway) \|\| ($.eventName=Delet eInternetGateway) || ($.eventN ame=DetachInternetGateway)}`
namespace de métrica	**`LogMetrics`**
Valor da métrica	**`1`**
Valor padrão	**`0`**

4. Criar um alarme com base no filtro Para obter instruções, consulte Criação de um CloudWatch alarme com base em um filtro métrico de grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Condições, tipo de limite	Estático
Sempre que *`your-metric-name`* for...	Maior/Igual
THAN	**`1`**

[CloudWatch.13] Certifique-se de que exista um filtro métrico de log e um alarme para alterações na tabela de rotas

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.13, CIS Foundations Benchmark v1.4.0/4.13 AWS

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso

AWS Config regra: Nenhuma (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se você monitora as chamadas de API em tempo real direcionando CloudTrail os CloudWatch registros para o Logs e estabelecendo filtros métricos e alarmes correspondentes. As tabelas de rotas encaminham o tráfego de rede entre sub-redes e gateways de rede.

Recomendamos que você crie um filtro de métrica e um alarme para fazer alterações em tabelas de rotas. Monitorar essas alterações ajuda a garantir que todo o tráfego da VPC passe por um caminho esperado.

> **Note**
>
> Quando o Security Hub executa a verificação desse controle, ele procura as CloudTrail trilhas que a conta atual usa. Essas trilhas podem ser trilhas da organização que pertencem a outra conta. As trilhas multirregionais também podem ser baseadas em uma região diferente.
> A verificação resulta em descobertas `FAILED` nos seguintes casos:
>
> - Nenhuma trilha está configurada.
> - As trilhas disponíveis que estão na região atual e que são de propriedade da conta atual não atendem aos requisitos de controle.
>
> A verificação resulta em um status de controle de `NO_DATA` nos seguintes casos:
>
> - As trilhas multirregionais também podem ser baseadas em uma região diferente. O Security Hub só pode gerar descobertas na região em que a trilha está baseada.
> - Uma trilha multirregional pertence a uma conta diferente. O Security Hub só pode gerar descobertas para a conta proprietária da trilha.
>
>   Recomendamos trilhas organizacionais para registrar eventos de logs de várias contas em uma organização. Por padrão, as trilhas da organização são trilhas multirregionais e só podem ser gerenciadas pela conta AWS Organizations de gerenciamento ou pela conta de administrador CloudTrail delegado. O uso de uma trilha organizacional resulta em um status de controle de `NO_DATA` aos controles avaliados nas contas dos membros da organização. Nas contas dos membros, o Security Hub só gera descobertas para recursos de propriedade dos membros. As descobertas relacionadas às trilhas da organização são geradas na conta do proprietário do recurso. É possível ver essas descobertas em sua conta de administrador delegado do Security Hub usando a agregação entre regiões.

Para o alarme, a conta atual deve ser proprietária do tópico do Amazon SNS referenciado ou deve ter acesso ao tópico do Amazon SNS chamando `ListSubscriptionsByTopic`. Caso contrário, o Security Hub gera descobertas de `WARNING` para o controle.

Correção

Note

Nosso padrão de filtro recomendado nessas etapas de correção difere do padrão de filtro na orientação do CIS. Nossos filtros recomendados têm como alvo somente eventos provenientes de chamadas de API do Amazon Elastic Computer Cloud (EC2).

Para passar por esse controle, siga estas etapas para criar um tópico do Amazon SNS, uma trilha de AWS CloudTrail , um filtro métrico e um alarme para o filtro métrico.

1. Criar um tópico do Amazon SNS. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service. Crie um tópico que receba todos os alarmes do CIS e crie pelo menos uma assinatura para o tópico.
2. Crie uma CloudTrail trilha que se aplique a todos Regiões da AWS. Para obter instruções, consulte Criação de um bucket no Guia do usuário do AWS CloudTrail (S3).

   Anote o nome do grupo de CloudWatch registros de registros que você associa à CloudTrail trilha. Você cria o filtro métrico para esse grupo de logs na próxima etapa.
3. Crie um filtro de métrica. Para obter instruções, consulte Criar um filtro métrico para um grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Definir padrão, padrão de filtro	`{($.eventSource=ec2.amazonaws.com) && (($.eventName=CreateRoute) || ($.eventName=CreateRouteTable) \|\| ($.eventName=ReplaceRoute) || ($.eventName=ReplaceRouteTableAssoci`

Campo	Valor
	`ation) || ($.eventName=Delet eRouteTable) \|\| ($.eventN ame=DeleteRoute) || ($.eventN ame=DisassociateRouteTable))}`
namespace de métrica	**`LogMetrics`**
Valor da métrica	**`1`**
Valor padrão	**`0`**

4. Criar um alarme com base no filtro Para obter instruções, consulte Criação de um CloudWatch alarme com base em um filtro métrico de grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Condições, tipo de limite	Estático
Sempre que *`your-metric-name`* for...	Maior/Igual
THAN	**`1`**

[CloudWatch.14] Certifique-se de que exista um filtro métrico de log e um alarme para alterações de VPC

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/3.14, CIS Foundations Benchmark v1.4.0/4.14 AWS

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso

AWS Config regra: Nenhuma (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Você pode monitorar em tempo real as chamadas de API direcionando CloudTrail os registros para o CloudWatch Logs e estabelecendo filtros métricos e alarmes correspondentes. É possível ter mais de uma VPC em uma conta e pode criar uma conexão de emparelhamento entre duas VPCs, permitindo que o tráfego de rede seja encaminhado entre VPCs.

Recomendamos que você crie um filtro de métrica e um alarme para fazer alterações em VPCs. Monitorar essas alterações ajuda a garantir que os controles de autenticação e autorização permaneçam intactos.

Para executar essa verificação, o Security Hub usa lógica personalizada para executar as etapas exatas de auditoria prescritas para o controle 4.14 no CIS AWS Foundations Benchmark v1.4.0. Haverá falha nesse controle se os filtros de métrica exatos prescritos pelo CIS não forem usados. Não é possível adicionar campos ou termos adicionais aos filtros de métrica.

Note

Quando o Security Hub executa a verificação desse controle, ele procura as CloudTrail trilhas que a conta atual usa. Essas trilhas podem ser trilhas da organização que pertencem a outra conta. As trilhas multirregionais também podem ser baseadas em uma região diferente.
A verificação resulta em descobertas `FAILED` nos seguintes casos:

- Nenhuma trilha está configurada.
- As trilhas disponíveis que estão na região atual e que são de propriedade da conta atual não atendem aos requisitos de controle.

A verificação resulta em um status de controle de `NO_DATA` nos seguintes casos:

- As trilhas multirregionais também podem ser baseadas em uma região diferente. O Security Hub só pode gerar descobertas na região em que a trilha está baseada.
- Uma trilha multirregional pertence a uma conta diferente. O Security Hub só pode gerar descobertas para a conta proprietária da trilha.

  Recomendamos trilhas organizacionais para registrar eventos de logs de várias contas em uma organização. Por padrão, as trilhas da organização são trilhas multirregionais e só podem ser gerenciadas pela conta AWS Organizations de gerenciamento ou pela conta de administrador CloudTrail delegado. O uso de uma trilha organizacional resulta em um status de controle de `NO_DATA` aos controles avaliados nas contas dos membros da

organização. Nas contas dos membros, o Security Hub só gera descobertas para recursos de propriedade dos membros. As descobertas relacionadas às trilhas da organização são geradas na conta do proprietário do recurso. É possível ver essas descobertas em sua conta de administrador delegado do Security Hub usando a agregação entre regiões.

Para o alarme, a conta atual deve ser proprietária do tópico do Amazon SNS referenciado ou deve ter acesso ao tópico do Amazon SNS chamando `ListSubscriptionsByTopic`. Caso contrário, o Security Hub gera descobertas de `WARNING` para o controle.

Correção

Para passar por esse controle, siga estas etapas para criar um tópico do Amazon SNS, uma trilha de AWS CloudTrail , um filtro métrico e um alarme para o filtro métrico.

1. Criar um tópico do Amazon SNS. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service. Crie um tópico que receba todos os alarmes do CIS e crie pelo menos uma assinatura para o tópico.
2. Crie uma CloudTrail trilha que se aplique a todos Regiões da AWS. Para obter instruções, consulte Criação de um bucket no Guia do usuário do AWS CloudTrail (S3).

   Anote o nome do grupo de CloudWatch registros de registros que você associa à CloudTrail trilha. Você cria o filtro métrico para esse grupo de logs na próxima etapa.
3. Crie um filtro de métrica. Para obter instruções, consulte Criar um filtro métrico para um grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Definir padrão, padrão de filtro	`{($.eventName=CreateVpc) \|\| ($.eventName=DeleteVpc) || ($.eventName=ModifyVpcAttribute) \|\| ($.eventName=AcceptVpcPeeringConnection) || ($.eventName=CreateVpcPeeringConnection) \|\| ($.eventName=DeleteVpcPeeringConnection) || ($.eventName=Rejec`

Campo	Valor
	`tVpcPeeringConnection) || ($.eventName=AttachClassicLinkVpc) \|\| ($.eventName=DetachClassicLinkVpc) || ($.eventName=DisableVpcClassicLink) \|\| ($.eventName=EnableVpcClassicLink)}`
namespace de métrica	**`LogMetrics`**
Valor da métrica	**`1`**
Valor padrão	**`0`**

4. Criar um alarme com base no filtro Para obter instruções, consulte Criação de um CloudWatch alarme com base em um filtro métrico de grupo de registros no Guia CloudWatch do usuário da Amazon. Use os seguintes valores:

Campo	Valor
Condições, tipo de limite	Estático
Sempre que *`your-metric-name`* for...	Maior/Igual
THAN	**`1`**

[CloudWatch.15] CloudWatch os alarmes devem ter ações especificadas configuradas

Categoria: Detectar > Serviços de detecção

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Severidade: alta

Tipo de recurso

AWS Config regra: **cloudwatch-alarm-action-check**

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`alarmActionRequired`	O controle produzirá uma descoberta `PASSED` se o parâmetro estiver definido como `true` e o alarme tiver uma ação quando o estado do alarme mudar para `ALARM`.	Booleano	Não personalizável	`true`
`insufficientDataActionRequired`	O controle produzirá uma descoberta `PASSED` se o parâmetro estiver definido como `true` e o alarme tiver uma ação quando o estado do alarme mudar para `INSUFFICIENT_DATA` .	Booleano	`true` ou `false`	`false`
`okActionRequired`	O controle produzirá uma descoberta `PASSED` se o parâmetro estiver definido como `true` e o alarme tiver uma ação quando o estado do alarme mudar para `OK`.	Booleano	`true` ou `false`	`false`

Esse controle verifica se um CloudWatch alarme da Amazon tem pelo menos uma ação configurada para o `ALARM` estado. O controle falhará se o alarme não tiver uma ação configurada para o estado `ALARM`. Opcionalmente, é possível incluir valores de parâmetros personalizados para também exigir ações de alarme para os estados `INSUFFICIENT_DATA` ou `OK`.

> **Note**
>
> O Security Hub avalia esse controle com base em alarmes CloudWatch métricos. Os alarmes métricos podem fazer parte de alarmes compostos que têm as ações especificadas configuradas. O controle gera `FAILED` descobertas nos seguintes casos:
>
> - As ações especificadas não estão configuradas para um alarme métrico.
> - O alarme métrico faz parte de um alarme composto que tem as ações especificadas configuradas.

Esse controle se concentra em saber se um CloudWatch alarme tem uma ação de alarme configurada, enquanto CloudWatch.17 se concentra no status de ativação de uma ação de CloudWatch alarme.

Recomendamos ações de CloudWatch alarme para alertá-lo automaticamente quando uma métrica monitorada estiver fora do limite definido. Os alarmes de monitoramento ajudam você a identificar atividades incomuns e a responder rapidamente a problemas operacionais e de segurança quando um alarme entra em um estado específico. O tipo de ação de alarme mais comum é notificar uma ou mais pessoas enviando uma mensagem a um tópico do Amazon Simple Notification Service (Amazon SNS).

Correção

Para obter informações sobre ações suportadas por CloudWatch alarmes, consulte Ações de alarme no Guia do CloudWatch usuário da Amazon.

[CloudWatch.16] os grupos de CloudWatch registros devem ser mantidos por um período de tempo especificado

Categoria: Identificar > Registro em log

Requisitos relacionados: NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-11, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-12

Severidade: média

Tipo de recurso

AWS Config regra: **`cw-loggroup-retention-period-check`**

Tipo de programação: Periódico

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub	
`minRetentionTime`	Período mínimo de retenção em dias para grupos de CloudWatch registros	Enum	`365`, `400`, `545`, `731`, `1827`, `3653`	`365`	

Esse controle verifica se um grupo de CloudWatch registros da Amazon tem um período de retenção de pelo menos o número especificado de dias. O controle falhará se o período de retenção for inferior ao número especificado. A menos que você forneça um valor de parâmetro personalizado para o período de retenção, o Security Hub usará um valor padrão de 365 dias.

CloudWatch Os registros centralizam os registros de todos os seus sistemas, aplicativos e Serviços da AWS em um único serviço altamente escalável. Você pode usar o CloudWatch Logs para monitorar, armazenar e acessar seus arquivos de log das instâncias do Amazon Elastic Compute Cloud (EC2) AWS CloudTrail, do Amazon Route 53 e de outras fontes. Manter seus logs por pelo menos 1 ano pode ajudá-lo a cumprir os padrões de retenção de logs.

Correção

Para definir as configurações de retenção de log, consulte Alterar retenção de dados de log em CloudWatch Logs no Guia CloudWatch do usuário da Amazon.

[CloudWatch.17] ações de CloudWatch alarme devem ser ativadas

Categoria: Detectar > Serviços de detecção

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Severidade: alta

Tipo de recurso

AWS Config regra: **`cloudwatch-alarm-action-enabled-check`**

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se as ações de CloudWatch alarme estão ativadas (`ActionEnabled`devem ser definidas como verdadeiras). O controle falhará se a ação de alarme de um CloudWatch alarme for desativada.

> **Note**
>
> O Security Hub avalia esse controle com base em alarmes CloudWatch métricos. Os alarmes métricos podem fazer parte de alarmes compostos que têm as ações de alarme ativadas. O controle gera `FAILED` descobertas nos seguintes casos:
>
> - As ações especificadas não estão configuradas para um alarme métrico.
> - O alarme métrico faz parte de um alarme composto que tem ações de alarme ativadas.

Esse controle se concentra no status de ativação de uma ação de CloudWatch alarme, enquanto CloudWatch.15 se concentra em saber se alguma `ALARM` ação está configurada em um CloudWatch alarme.

Recomendamos ativar as ações de alarme para alertá-lo automaticamente quando uma métrica monitorada estiver fora do limite definido. Se a ação de alarme for desativada, nenhuma ação será executada quando o alarme mudar de estado, e você não será alertado sobre alterações nas métricas monitoradas. Recomendamos ativar as ações de CloudWatch alarme para ajudá-lo a responder rapidamente aos problemas operacionais e de segurança.

Correção

Para ativar uma ação CloudWatch de alarme (console)

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Alarms (Alarmes), All alarms (Todos os alarmes).

3. Selecione o alarme para o qual você deseja ativar as ações.
4. Em Ações, escolha Ações de alarme — novas e, em seguida, escolha Ativar.

Para obter mais informações sobre a ativação de ações de CloudWatch alarme, consulte Ações de alarme no Guia do CloudWatch usuário da Amazon.

AWS CodeArtifact controles

Esses controles estão relacionados aos CodeArtifact recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[CodeArtifact.1] CodeArtifact repositórios devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-codeartifact-repository` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um AWS CodeArtifact repositório tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o repositório não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o repositório não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um CodeArtifact repositório, consulte Marcar um repositório CodeArtifact no Guia do AWS CodeArtifact usuário.

AWS CodeBuild controles

Esses controles estão relacionados aos CodeBuild recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais

Requisitos relacionados: PCI DSS v3.2.1/8.2.1, NIST.800-53.r5 SA-3

Categoria: Proteger > Desenvolvimento seguro

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `codebuild-project-source-repo-url-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o URL do repositório de origem do Bitbucket do AWS CodeBuild projeto contém tokens de acesso pessoais ou um nome de usuário e senha. O controle falhará se o URL do repositório de origem do Bitbucket contiver tokens de acesso pessoais ou um nome de usuário e senha.

> **Note**
>
> Esse controle avalia a fonte primária e as fontes secundárias de um projeto de CodeBuild compilação. Para obter mais informações sobre fontes do projeto, consulte Exemplo de várias fontes de entrada e artefatos de saída no Guia do AWS CodeBuild usuário.

As credenciais de login não devem ser armazenadas ou transmitidas em texto não criptografado nem aparecer na URL do repositório de origem. Em vez de tokens de acesso pessoal ou credenciais de login, você deve acessar seu provedor de origem e alterar a URL do repositório de origem para conter somente o caminho para a localização do repositório Bitbucket. CodeBuild O uso de tokens de acesso pessoal ou credenciais de login pode resultar em exposição não intencional de dados ou acesso não autorizado.

Correção

Você pode atualizar seu CodeBuild projeto para usar o OAuth.

Para remover a autenticação básica/(GitHub) Personal Access Token da fonte do CodeBuild projeto

1. Abra o CodeBuild console em https://console.aws.amazon.com/codebuild/.
2. Escolha o projeto de compilação que contém tokens de acesso pessoal ou um nome de usuário e uma senha.
3. Em Edit (Editar), selecione Source (Origem).
4. Escolha Desconectar de GitHub /Bitbucket.
5. Escolha Connect using OAuth e, em seguida, escolha Connect to GitHub/Bitbucket.
6. Quando solicitado, escolha authorize as appropriate (autorizar conforme apropriado).
7. Redefina as configurações de URL do repositório e configuração adicional, conforme necessário.
8. Selecione Update source (Atualizar origem).

Para obter mais informações, consulte exemplos baseados em casos de CodeBuild uso no Guia do AWS CodeBuild usuário.

[CodeBuild.2] as variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado

Requisitos relacionados: PCI DSS v3.2.1/8.2.1, NIST.800-53.r5 SA-3

Categoria: Proteger > Desenvolvimento seguro

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `codebuild-project-envvar-awscred-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Este controle verifica se o projeto contém as variáveis de ambiente `AWS_ACCESS_KEY_ID` e `AWS_SECRET_ACCESS_KEY`.

As credenciais de autenticação `AWS_ACCESS_KEY_ID` e `AWS_SECRET_ACCESS_KEY` nunca devem ser armazenadas em texto não criptografado, pois isso poderia levar à exposição não intencional de dados e acesso não autorizado.

Correção

Para remover variáveis de ambiente de um CodeBuild projeto, consulte Alterar as configurações de um projeto de compilação AWS CodeBuild no Guia AWS CodeBuild do usuário. Certifique-se de que nada esteja selecionado para as Variáveis de ambiente.

Você pode armazenar variáveis de ambiente com valores confidenciais no AWS Systems Manager Parameter Store ou AWS Secrets Manager recuperá-las de sua especificação de compilação. Para obter instruções, consulte a caixa chamada Importante na seção Ambiente do Guia do usuário do AWS CodeBuild .

[CodeBuild.3] Os registros do CodeBuild S3 devem ser criptografados

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `codebuild-project-s3-logs-encrypted`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os registros do Amazon S3 de um AWS CodeBuild projeto estão criptografados. O controle falhará se a criptografia for desativada para os registros do S3 de um CodeBuild projeto.

A criptografia de dados em repouso é uma prática recomendada para adicionar uma camada de gerenciamento de acesso aos seus dados. Criptografar os registros em repouso reduz o risco de um usuário não autenticado acessar AWS os dados armazenados no disco. Ele adiciona outro conjunto de controles de acesso para limitar a capacidade de usuários não autorizados acessarem os dados.

Correção

Para alterar as configurações de criptografia dos registros CodeBuild do projeto S3, consulte Alterar as configurações de um projeto de compilação AWS CodeBuild no Guia do AWS CodeBuild usuário.

[CodeBuild.4] ambientes de CodeBuild projeto devem ter uma duração de registro AWS Config

Requisitos relacionados: CIS Foundations Benchmark v1.2.0/2.1, CIS Foundations Benchmark v1.4.0/3.1, NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-14(1), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8), NIST.800-53.r5 SA-8(22)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `codebuild-project-logging-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um ambiente de CodeBuild projeto tem pelo menos uma opção de log, seja para S3 ou para CloudWatch logs habilitados. Esse controle falhará se um ambiente de CodeBuild projeto não tiver pelo menos uma opção de log ativada.

Do ponto de vista da segurança, o registro em log é um atributo importante para permitir futuros esforços forenses no caso de incidentes de segurança. Correlacionar anomalias em CodeBuild projetos com detecções de ameaças pode aumentar a confiança na precisão dessas detecções de ameaças.

Correção

Para obter mais informações sobre como definir as configurações CodeBuild do registro do projeto, consulte Criar um projeto de compilação (console) no Guia CodeBuild do usuário.

[CodeBuild.5] ambientes de CodeBuild projeto não devem ter o modo privilegiado ativado

> **Important**
>
> O Security Hub retirou esse controle em abril de 2024. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: alta

Tipo de recurso

Regra do AWS Config : `codebuild-project-environment-privileged-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um ambiente de AWS CodeBuild projeto tem o modo privilegiado ativado ou desativado. O controle falhará se um ambiente de CodeBuild projeto tiver o modo privilegiado ativado.

Por padrão, os contêineres do Docker não permitem acesso a nenhum dispositivo. O modo privilegiado concede acesso a contêiner Docker de um projeto de compilação a todos os dispositivos. A configuração `privilegedMode` com valor `true` permite que o daemon do Docker seja executado dentro de um contêiner do Docker. O daemon do Docker escuta as solicitações da API do Docker e gerencia objetos do Docker, como imagens, contêineres, redes e volumes. Defina como true somente se o projeto de compilação for usado para criar imagens de Docker. Caso contrário, essa configuração deve ser desativada para impedir o acesso não intencional às APIs do Docker, bem como ao hardware subjacente do contêiner. A configuração de `privilegedMode` para `false` ajuda a proteger recursos essenciais contra adulteração e exclusão.

Correção

Para definir as configurações do ambiente do CodeBuild projeto, consulte Criar um projeto de compilação (console) no Guia CodeBuild do usuário. Na seção Ambiente, não selecione a configuração Privilegiada.

AWS Config controles

Esses controles estão relacionados aos AWS Config recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[Config.1] AWS Config deve estar habilitado

Requisitos relacionados: PCI DSS v3.2.1/10.5.2, PCI DSS v3.2.1/11.5, CIS Foundations Benchmark v1.2.0/2.5, CIS Foundations Benchmark v1.4.0/3.5, CIS AWS Foundations Benchmark v3.0.0/3.3, NIST.800-53.r5 CM-3, NIST.800-53.r5 CM-6 (1), NIST.800-53.r5 M-8, AWS Nist.800-53.R5 CM-8 (2) AWS

Categoria: Identificar > Inventário

Severidade: média

Tipo de recurso

AWS Config regra: Nenhuma (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se AWS Config está ativado em sua conta na região atual e se está registrando todos os recursos. O controle falhará se AWS Config não estiver ativado ou não estiver registrando todos os recursos.

O AWS Config serviço executa o gerenciamento da configuração dos AWS recursos compatíveis em sua conta e entrega arquivos de log para você. As informações registradas incluem o item de configuração (AWS recurso), os relacionamentos entre os itens de configuração e quaisquer alterações de configuração entre os recursos.

O Security Hub recomenda que você habilite AWS Config em todas as regiões. O histórico do item de AWS configuração que AWS Config captura permite a análise de segurança, o rastreamento de alterações de recursos e a auditoria de conformidade.

> **Note**
>
> O Config.1 exige que AWS Config esteja habilitado em todas as regiões nas quais você usa o Security Hub.
> Como o é um serviço regional, a verificação realizada nesse controle verifica somente a região atual da conta. Ele não verifica todas as Regiões.
> Para que as verificações de segurança de recursos globais de cada região possam ser realizadas, é necessário registrar os recursos globais. Se você registrar apenas recursos globais em uma única região, poderá desabilitar esse controle em todas as regiões, exceto na região em que registra recursos globais.
> Os tipos de recursos registrados globalmente que AWS Config oferecem suporte são usuários, grupos, funções e políticas gerenciadas pelo cliente do IAM. É possível considerar a desativação dos controles do Security Hub que verificam esses tipos de recursos em regiões onde a gravação global de recursos está desativada. Como o IAM é um serviço global, os recursos do IAM só serão registrados na região em que o registro global de recursos está ativado. Para ter mais informações, consulte Controles do Security Hub que podem ser desabilitados.

Correção

Para habilitá-lo AWS Config e configurá-lo para registrar todos os recursos, consulte Configuração manual no Guia do AWS Config desenvolvedor. Para registrar recursos globais e garantir que nenhum tipo de recurso seja excluído, selecione Todos os recursos com substituições personalizáveis. Remova todas as configurações de substituição e defina a frequência de gravação para Gravação contínua.

Você também pode usar um AWS CloudFormation modelo para automatizar esse processo. Para obter mais informações, consulte os modelos de AWS CloudFormation StackSets amostra no Guia AWS CloudFormation do usuário.

Controles do Amazon Data Firehose

Esses controles estão relacionados aos recursos do Amazon Data Firehose.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso

Requisitos relacionados: NIST.800-53.r5 AC-3, NIST.800-53.r5 AU-3, Nist.800-53.r5 SC-12, NIST.800-53.r5 SC-13, Nist.800-53.r5 SC-28

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra do AWS Config : `kinesis-firehose-delivery-stream-encrypted`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um stream de entrega do Amazon Data Firehose está criptografado em repouso com criptografia do lado do servidor. Esse controle falhará se um stream de entrega do Firehose não for criptografado em repouso com criptografia do lado do servidor.

A criptografia do lado do servidor é um recurso nos fluxos de entrega do Amazon Data Firehose que criptografa automaticamente os dados antes que estejam em repouso usando uma chave criada em (). AWS Key Management Service AWS KMS Os dados são criptografados antes de serem gravados na camada de armazenamento de stream Data Firehose e descriptografados após serem recuperados do armazenamento. Isso permite que você cumpra os requisitos regulamentares e aumente a segurança de seus dados.

Correção

Para habilitar a criptografia do lado do servidor nos fluxos de entrega do Firehose, consulte Proteção de dados no Amazon Data Firehose no Guia do desenvolvedor do Amazon Data Firehose.

Controles do Amazon Detective

Esses controles estão relacionados aos recursos do Detective.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[Detetive.1] Os gráficos do comportamento do detetive devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-detective-graph` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um gráfico de comportamento do Amazon Detective tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o gráfico de comportamento não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o gráfico de comportamento não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou

outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um gráfico de comportamento de Detective, consulte Adicionar tags a um gráfico de comportamento no Amazon Detective Administration Guide.

AWS Database Migration Service controles

Esses controles estão relacionados aos AWS DMS recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

As instâncias de replicação do PCI.DMS.1 Database Migration Service não devem ser públicas

Requisitos relacionados: PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/1.3.2,PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

Categoria: Proteger > Configuração de rede segura

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `dms-replication-not-public`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se AWS DMS as instâncias de replicação são públicas. Para fazer isso, ele examina o valor do campo `PubliclyAccessible`.

Uma instância de replicação privada tem um endereço IP privado que não pode ser acessado fora da rede de replicação. Uma instância de replicação deve ter um endereço IP privado quando os bancos de dados de origem e de destino ficam na mesma rede que está conectada ao VPC da instância de replicação usando VPN, ou emparelhamento de VPC. A rede também deve estar conectada à VPC da instância de replicação usando uma VPN AWS Direct Connect ou emparelhamento de VPC. Para saber mais sobre instâncias de replicação públicas e privadas, consulte Instâncias de replicação públicas e privadas no Guia do usuário do AWS Database Migration Service .

Você também deve garantir que o acesso à configuração da sua AWS DMS instância seja limitado somente aos usuários autorizados. Para fazer isso, restrinja as permissões do IAM dos usuários para modificar AWS DMS configurações e recursos.

Correção

Você não pode alterar a configuração de acesso público de uma instância de replicação do DMS depois de criá-la. Para alterar a configuração de acesso público, exclua sua instância atual e, em seguida, recrie-a. Não selecione a opção Acessível ao público.

[DMS.2] Os certificados DMS devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-dms-certificate` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um AWS DMS certificado tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o certificado não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o certificado não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive

AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um certificado DMS, consulte Como marcar recursos AWS Database Migration Service no Guia do AWS Database Migration Service usuário.

[DMS.3] As assinaturas de eventos do DMS devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-dms-eventsubscription` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se uma assinatura de AWS DMS evento tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a assinatura do evento não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle verificará apenas a existência de uma chave de tag e falhará se a assinatura do evento não estiver

marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com `aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma assinatura de evento do DMS, consulte Como marcar recursos AWS Database Migration Service no Guia do AWS Database Migration Service usuário.

[DMS.4] As instâncias de replicação do DMS devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-dms-replicationinstance` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se uma instância AWS DMS de replicação tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a instância de replicação não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a instância de replicação não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive

AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma instância de replicação do DMS, consulte Como marcar recursos AWS Database Migration Service no Guia do AWS Database Migration Service usuário.

[DMS.5] Os grupos de sub-redes de replicação do DMS devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-dms-replicationsubnetgroup` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um grupo AWS DMS de sub-redes de replicação tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o grupo de sub-redes

de replicação não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro. `requiredTagKeys` Se o parâmetro `requiredTagKeys` não for fornecido, o controle somente verificará a existência de uma chave de tag e falhará se o grupo de sub-redes de replicação não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um grupo de sub-redes de replicação do DMS, consulte Como marcar recursos AWS Database Migration Service no Guia do usuário.AWS Database Migration Service

As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Detectar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: média

Tipo de recurso

Regra do AWS Config : dms-auto-minor-version-upgrade-check

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se a atualização automática de versões secundárias está habilitada para uma instância de AWS DMS replicação. Esse controle verifica se a atualização automática de versões secundárias está habilitada para uma instância de replicação do .

O DMS fornece atualização automática de versões secundárias para cada mecanismo de replicação compatível para que você possa manter sua instância de replicação. up-to-date Versões secundárias podem introduzir novos atributos de software, correções de bugs, patches de segurança e melhorias de desempenho. Ao habilitar a atualização automática de versões secundárias em instâncias de replicação do DMS, atualizações menores são aplicadas automaticamente durante a janela de manutenção ou imediatamente se a opção Aplicar alterações imediatamente for escolhida.

Correção

Para habilitar a atualização automática de versões secundárias em instâncias de replicação do DMS, consulte Modificar uma instância de replicação no Guia do usuário do AWS Database Migration Service .

As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : dms-replication-task-targetdb-logging

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o registro em log está habilitado com o nível mínimo de severidade de `LOGGER_SEVERITY_DEFAULT` para as tarefas de replicação do DMS `TARGET_APPLY` e `TARGET_LOAD`. O controle falhará se o registro em log não estiver habilitado para essas tarefas ou se o nível mínimo de severidade for menor que `LOGGER_SEVERITY_DEFAULT`.

O DMS usa CloudWatch a Amazon para registrar informações durante o processo de migração. Usando as configurações de tarefa de registro em log, é possível especificar quais atividades de componente serão registradas em log e quantas informações serão registradas no log. Você deve especificar o registro em log das seguintes tarefas:

- TARGET_APPLY as instruções de dados e linguagem de definição de dados (DDL) são aplicadas ao banco de dados de destino.
- `TARGET_LOAD` — Os dados são carregados no banco de dados de destino.

O registro em log desempenha um papel fundamental nas tarefas de replicação do DMS, permitindo monitoramento, solução de problemas, auditoria, análise de desempenho, detecção e recuperação de erros, bem como análises e relatórios históricos. Ele ajuda a garantir a replicação bem-sucedida de dados entre bancos de dados, mantendo a integridade dos dados e a conformidade com os requisitos normativos. Níveis de registro em log diferentes de `DEFAULT` raramente são necessários para esses componentes durante a solução de problemas. Recomendamos manter o nível de registro em log como `DEFAULT` para esses componentes, a menos que seja especificamente solicitado alterá-lo por AWS Support. Um nível mínimo de registro em log de `DEFAULT` garante que mensagens informativas, avisos e mensagens de erro sejam gravadas nos logs. Esse controle verifica se o nível de registro em log é pelo menos um dos seguintes para as tarefas de replicação anteriores: `LOGGER_SEVERITY_DEFAULT`, `LOGGER_SEVERITY_DEBUG` ou `LOGGER_SEVERITY_DETAILED_DEBUG`.

Correção

Para ativar o registro em log para tarefas de replicação do DMS do banco de dados de destino, consulte Visualização e gerenciamento de registros de AWS DMS tarefas no Guia do AWS Database Migration Service usuário.

As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `dms-replication-task-sourcedb-logging`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o registro em log está habilitado com o nível mínimo de severidade de `LOGGER_SEVERITY_DEFAULT` para as tarefas de replicação do DMS `SOURCE_CAPTURE` e `SOURCE_UNLOAD`. O controle falhará se o registro em log não estiver habilitado para essas tarefas ou se o nível mínimo de severidade for menor que `LOGGER_SEVERITY_DEFAULT`.

O DMS usa CloudWatch a Amazon para registrar informações durante o processo de migração. Usando as configurações de tarefa de registro em log, é possível especificar quais atividades de componente serão registradas em log e quantas informações serão registradas no log. É possível especificar o registro em log das seguintes ações:

- `SOURCE_CAPTURE` — Os dados de replicação contínua ou captura de dados de alteração (CDC) são capturados do banco de dados ou serviço de origem e passados para o componente de serviço `SORTER`.
- `SOURCE_UNLOAD` — Os dados são descarregados do banco de dados ou serviço de origem durante a carga total.

O registro em log desempenha um papel fundamental nas tarefas de replicação do DMS, permitindo monitoramento, solução de problemas, auditoria, análise de desempenho, detecção e recuperação de erros, bem como análises e relatórios históricos. Ele ajuda a garantir a replicação bem-sucedida de dados entre bancos de dados, mantendo a integridade dos dados e a conformidade com os requisitos normativos. Níveis de registro em log diferentes de `DEFAULT` raramente

são necessários para esses componentes durante a solução de problemas. Recomendamos manter o nível de registro em log como `DEFAULT` para esses componentes, a menos que seja especificamente solicitado alterá-lo por AWS Support. Um nível mínimo de registro em log de `DEFAULT` garante que mensagens informativas, avisos e mensagens de erro sejam gravadas nos logs. Esse controle verifica se o nível de registro em log é pelo menos um dos seguintes para as tarefas de replicação anteriores: `LOGGER_SEVERITY_DEFAULT`, `LOGGER_SEVERITY_DEBUG` ou `LOGGER_SEVERITY_DETAILED_DEBUG`.

Correção

Para habilitar o registro em log para tarefas de replicação do DMS do banco de dados de origem, consulte Visualização e gerenciamento de registros de AWS DMS tarefas no Guia do AWS Database Migration Service usuário.

Os endpoints do DMS devem usar SSL

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Criptografia de data-in-transit

Severidade: média

Tipo de recurso

Regra do AWS Config : `dms-endpoint-ssl-configured`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um AWS DMS endpoint usa uma conexão SSL. O controle falhará se o endpoint não usar SSL.

As conexões SSL/TLS fornecem uma camada de segurança criptografando dados que se movem entre o cliente e a instânciao cluster de banco de dados. O uso de um certificado de servidor fornece uma camada extra de segurança, validando se a conexão está sendo feita comuma instânciaum cluster de banco de dados do . Para isso, ele verifica o certificado de servidor que é instalado automaticamente em todas as instânciastodos os clusters de banco de dados que você provisiona. Ao habilitar a conexão SSL em seus endpoints do DMS, você protege a confidencialidade dos dados durante a migração.

Correção

Para adicionar uma conexão SSL a um endpoint do DMS novo ou existente, consulte Usar SSL com AWS Database Migration Service no Guia do usuário do AWS Database Migration Service .

[DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada

Requisitos relacionados: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-6, Nist.800-53.r5 AC-17, NIST.800-53.r5 IA-2, Nist.800-53.r5 IA-5

Categoria: Proteger > Gerenciamento de acesso seguro > Autenticação sem senha

Severidade: média

Tipo de recurso

Regra do AWS Config : `dms-neptune-iam-authorization-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um AWS DMS endpoint para um banco de dados Amazon Neptune está configurado com autorização do IAM. O controle falhará se o endpoint do DMS não tiver a autorização do IAM habilitada.

AWS Identity and Access Management (IAM) fornece controle de acesso refinado em toda parte. AWS Com o IAM, você pode especificar quem pode acessar quais serviços e recursos e sob quais condições. Com as políticas do IAM, você gerencia as permissões para sua força de trabalho e sistemas para garantir permissões com privilégios mínimos. Ao habilitar a autorização do IAM em AWS DMS endpoints para bancos de dados Neptune, você pode conceder privilégios de autorização aos usuários do IAM usando uma função de serviço especificada pelo parâmetro. `ServiceAccessRoleARN`

Correção

Para habilitar a autorização do IAM em endpoints do DMS para bancos de dados Neptune, consulte Como usar o Amazon Neptune como destino no Guia do usuário. AWS Database Migration ServiceAWS Database Migration Service

[DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado

Requisitos relacionados: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-6, Nist.800-53.r5 IA-2, Nist.800-53.r5 IA-5

Categoria: Proteger > Gerenciamento de acesso seguro > Autenticação sem senha

Severidade: média

Tipo de recurso

Regra do AWS Config : `dms-mongo-db-authentication-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um AWS DMS endpoint para o MongoDB está configurado com um mecanismo de autenticação. O controle falhará se um tipo de autenticação não estiver definido para o endpoint.

AWS Database Migration Service suporta dois métodos de autenticação para MongoDB — MONGODB-CR para MongoDB versão 2.x e SCRAM-SHA-1 para MongoDB versão 3.x ou posterior. Esses métodos de autenticação são usados para autenticar e criptografar senhas do MongoDB se os usuários quiserem usar as senhas para acessar os bancos de dados. A autenticação em AWS DMS endpoints garante que somente usuários autorizados possam acessar e modificar os dados que estão sendo migrados entre bancos de dados. Sem a autenticação adequada, usuários não autorizados podem obter acesso a dados confidenciais durante o processo de migração. Isso pode resultar em violações de dados, perda de dados ou outros incidentes de segurança.

Correção

Para habilitar um mecanismo de autenticação nos endpoints do DMS para o MongoDB, consulte Usando o MongoDB como fonte no Guia do Usuário. AWS DMSAWS Database Migration Service

[DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado

Requisitos relacionados: NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-13

Categoria: Proteger > Proteção de dados > Criptografia de dados em trânsito

Severidade: média

Tipo de recurso

Regra do AWS Config : `dms-redis-tls-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um AWS DMS endpoint para Redis está configurado com uma conexão TLS. O controle falhará se o endpoint não tiver o TLS ativado.

O TLS fornece end-to-end segurança quando os dados são enviados entre aplicativos ou bancos de dados pela Internet. Quando você configura a criptografia SSL para seu endpoint DMS, ela permite a comunicação criptografada entre os bancos de dados de origem e de destino durante o processo de migração. Isso ajuda a evitar a espionagem e a interceptação de dados confidenciais por agentes mal-intencionados. Sem a criptografia SSL, dados confidenciais podem ser acessados, resultando em violações de dados, perda de dados ou outros incidentes de segurança.

Correção

Para habilitar uma conexão TLS em endpoints DMS para Redis, consulte Usando o Redis como destino no Guia do usuário. AWS Database Migration ServiceAWS Database Migration Service

Controles do Amazon DocumentDB

Esses controles estão relacionados aos recursos do Amazon DocumentDB.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

Os clusters do Amazon DocumentDB devem ser criptografados em repouso

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra do AWS Config : docdb-cluster-encrypted

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster do Amazon DocumentDB é criptografado em repouso. Esse controle verifica se um cluster do Amazon DocumentDB é criptografado em repouso.

Dados em repouso se referem a qualquer dado armazenado em armazenamento persistente e não volátil por qualquer período. A criptografia ajuda a proteger a confidencialidade desses dados, reduzindo o risco de que um usuário não autorizado possa acessá-los. Os dados nos clusters do Amazon DocumentDB devem ser criptografados em repouso para uma camada adicional de segurança. O Amazon DocumentDB usa o Advanced Encryption Standard de 256 bits (AES-256) para criptografar seus dados usando chaves de criptografia armazenadas em AWS Key Management Service (AWS KMS).

Correção

É possível ativar a criptografia em repouso ao criar um cluster do Amazon DocumentDB. Não é possível alterar as configurações de criptografia após a criação de um cluster. Para obter mais informações, consulte Usar fluxos de alterações com o Amazon DocumentDB no Guia do desenvolvedor do Amazon DocumentDB.

Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado

Requisitos relacionados: NIST.800-53.r5 CA-7

Categoria: Recuperação > Resiliência > Backups ativados

Severidade: média

Tipo de recurso

Regra do AWS Config : docdb-cluster-backup-retention-check

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub	
`minimumBackupRetentionPeriod`	Período mínimo de retenção de backups em dias	Inteiro	7 para 35	7	

Esse controle verifica se um cluster do Amazon DocumentDB tem um período de retenção de backup maior ou igual ao período de tempo especificado. O controle falhará se o período de retenção de backup for inferior ao período de tempo especificado. A menos que você forneça um valor de parâmetro personalizado para o período de retenção do backup, o Security Hub usará um valor padrão de 7 dias.

Os backups ajudam você a se recuperar mais rapidamente de um incidente de segurança e a fortalecer a resiliência de seus sistemas. Ao automatizar backups para seus clusters do Amazon DocumentDB, será possível restaurar seus sistemas em um determinado momento e minimizar o tempo de inatividade e a perda de dados. No Amazon DocumentDB, os clusters têm um período de retenção de backup padrão de 1 dia. Isso deve ser aumentado para um valor entre 7 e 35 dias para passar por esse controle.

Correção

Para alterar o período de retenção de backup para seus clusters do Amazon DocumentDB, consulte Modificar um cluster do Amazon DocumentDB no Guia do desenvolvedor do Amazon DocumentDB. Em Backup, escolha o período de retenção de backup.

Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Configuração de rede segura

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `docdb-cluster-snapshot-public-prohibited`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um instantâneo de cluster manual do Amazon DocumentDB é público. O controle falhará se o instantâneo manual do cluster for público.

Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos Se você compartilhar um instantâneo manual não criptografado como público, isso o disponibilizará para todas as contas da AWS. Instantâneos públicos podem resultar em exposição não intencional de dados.

> **Note**
>
> Esse controle avalia os instantâneos manuais do cluster. Você não pode compartilhar um instantâneo de cluster automatizado do Amazon DocumentDB. Como alternativa, crie um instantâneo manual copiando o instantâneo automatizado e compartilhe essa cópia.

Correção

Para remover o acesso público aos instantâneos manuais do cluster do Amazon DocumentDB, consulte Compartilhar um instantâneo no Guia do desenvolvedor do Amazon DocumentDB. Programaticamente, é possível usar a operação Amazon DocumentDB `modify-db-snapshot-attribute`. Defina `restore` como `values-to-remove` e como

[DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : docdb-cluster-audit-logging-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster do Amazon DocumentDB publica logs de auditoria no Amazon Logs. CloudWatch O controle falhará se o cluster não publicar registros de auditoria no CloudWatch Logs.

Com o Amazon DocumentDB (compatível com MongoDB), é possível auditar eventos que foram realizados em seu cluster. Exemplos de eventos registrados incluem tentativas de autenticação bem-sucedidas e com falha, eliminação de uma coleção em um banco de dados ou criação de um índice. Por padrão, a auditoria está desativada no Amazon DocumentDB e exige que você tome medidas para habilitá-la.

Correção

Para publicar os logs de auditoria do Amazon DocumentDB no Logs, consulte Habilitar a CloudWatch auditoria no Guia do desenvolvedor do Amazon DocumentDB.

Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Proteger > Proteção de dados > Proteção contra exclusão de dados

Severidade: média

Tipo de recurso

Regra do AWS Config : docdb-cluster-deletion-protection-enabled

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster do Amazon DocumentDB tem a proteção contra exclusão habilitada. O controle falhará se o cluster não tiver a proteção contra exclusão habilitada.

A ativação da proteção contra exclusão de clusters oferece uma camada adicional de proteção contra a exclusão acidental do banco de dados ou a exclusão por um usuário não autorizado. Um cluster do Amazon DocumentDB não pode ser excluído enquanto a proteção contra exclusão está habilitada. Primeiro, você deve desativar a proteção contra exclusão para que uma solicitação de exclusão possa ser bem-sucedida. A proteção contra exclusão está habilitada por padrão ao criar um cluster usando o console.

Correção

Para alterar o período de retenção de backup para seus clusters do Amazon DocumentDB, consulte Modificar um cluster do Amazon DocumentDB no Guia do desenvolvedor do Amazon DocumentDB. Na seção Modificar cluster, escolha Habilitar para Proteção contra exclusão.

Controles do Amazon DynamoDB

Esses controles estão relacionados aos recursos da API de Gateway.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

As tabelas do DynamoDB devem escalar automaticamente a capacidade de acordo com a demanda

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra do AWS Config : `dynamodb-autoscaling-enabled`

Tipo de programação: Periódico

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados válidos	Valor padrão do Security Hub
`minProvisionedReadCapacity`	Número mínimo de unidades de capacidade de leitura provisionada para o ajuste de escala automático	Inteiro	1 para `40000`	Nenhum valor padrão
`targetReadUtilization`	Percentual de utilização pretendida para a capacidade de leitura	Inteiro	`20` para `90`	Nenhum valor padrão
`minProvisionedWriteCapacity`	Número mínimo de unidades de capacidade de gravação provisionada para o ajuste de escala automático	Inteiro	1 para `40000`	Nenhum valor padrão
`targetWriteUtilization`	Percentual de utilização pretendida para a capacidade de gravação	Inteiro	`20` para `90`	Nenhum valor padrão

Esse controle verifica se uma tabela do Amazon DynamoDB pode escalar sua capacidade de leitura e gravação conforme necessário. O controle falhará se a tabela não usar o modo de capacidade sob demanda ou o modo provisionado com ajuste de escala automático configurado. Por padrão, esse controle exige apenas que um desses modos seja configurado, independentemente dos níveis específicos de capacidade de leitura ou gravação. Opcionalmente, é possível fornecer valores de parâmetros personalizados para exigir níveis específicos de capacidade de leitura e gravação ou de utilização desejada.

A escalabilidade da capacidade com a demanda evita exceções de controle de utilização, o que ajuda a manter a disponibilidade de seus aplicativos. As tabelas do DynamoDB no modo de capacidade sob demanda são limitadas apenas pelas cotas de tabela padrão de throughput do DynamoDB. Para aumentar essas cotas, você pode registrar um ticket de suporte com AWS Support tabelas.DynamoDB no modo provisionado com escalabilidade automática e ajustar dinamicamente a capacidade de taxa de transferência provisionada em resposta aos padrões de tráfego. Para obter mais informações sobre o controle de utilização de solicitações do DynamoDB, consulte Controle

de utilização de solicitações e capacidade de expansão no Guia do desenvolvedor do Amazon DynamoDB.

Correção

Para habilitar a escalabilidade automática do DynamoDB em tabelas existentes no modo de capacidade, consulte Ativar o ajuste de escala automático do DynamoDB no Guia do desenvolvedor do Amazon DynamoDB.

[DynamoDB.2] As tabelas do DynamoDB devem ter a recuperação ativada point-in-time

Requisitos relacionados: NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-11, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-12

Categoria: Recuperação > Resiliência > Backups ativados

Severidade: média

Tipo de recurso

Regra do AWS Config : `dynamodb-pitr-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se a point-in-time recuperação (PITR) está habilitada para uma tabela do Amazon DynamoDB.

Os backups ajudam você a se recuperar mais rapidamente de um incidente de segurança. Eles também fortalecem a resiliência de seus sistemas. A recuperação do point-in-time DynamoDB automatiza os backups das tabelas do DynamoDB. Ele reduz o tempo de recuperação de operações acidentais de exclusão ou gravação. As tabelas do DynamoDB que têm a PITR habilitada podem ser restauradas para qualquer ponto nos últimos 35 dias.

Correção

Para restaurar uma tabela do DynamoDB em um determinado momento, consulte Restaurar uma tabela do DynamoDB para um ponto no tempo no Guia do desenvolvedor do Amazon DynamoDB.

Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra do AWS Config : `dax-encryption-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um cluster do Amazon DocumentDB é criptografado em repouso.

Criptografar dados em repouso reduz o risco de os dados armazenados em disco serem acessados por um usuário não autenticado. AWS Ele adiciona outro conjunto de controles de acesso para limitar a capacidade de usuários não autorizados acessarem os dados. Por exemplo, as permissões da API são necessárias para descriptografar os dados antes que eles possam ser lidos.

Correção

Não é possível ativar ou desativar a criptografia em repouso após a criação e um cluster. É necessário recriar o cluster para habilitar a criptografia em repouso. Para obter instruções detalhadas sobre como criar um cluster DAX com a criptografia em repouso ativada, consulte Ativar criptografia em repouso usando o AWS Management Console no Guia do desenvolvedor do Amazon DynamoDB.

As tabelas do DynamoDB devem estar presentes em um plano de backup

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Recuperação > Resiliência > Backups ativados

Severidade: média

Tipo de recurso

AWS Config regra: **dynamodb-resources-protected-by-backup-plan**

Tipo de programação: Periódico

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`backupVaultLockCheck`	O controle produz uma `PASSED` descoberta se o parâmetro estiver definido como `true` e o recurso usar o AWS Backup Vault Lock.	Booleano	`true` ou `false`	Nenhum valor padrão

Esse controle avalia se uma tabela do Amazon DynamoDB no estado `ACTIVE` está coberta por um plano de backup. O controle falhará se a tabela do DynamoDB não estiver coberta por um plano de backup. Se você definir o `backupVaultLockCheck` parâmetro igual `atrue`, o controle passará somente se o backup da tabela do DynamoDB for feito em AWS Backup um cofre bloqueado.

AWS Backup é um serviço de backup totalmente gerenciado que ajuda você a centralizar e automatizar o backup de dados em todo lugar. Serviços da AWS Com AWS Backup, você pode criar planos de backup que definam seus requisitos de backup, como com que frequência fazer backup de seus dados e por quanto tempo mantê-los. Incluir tabelas do DynamoDB em seus planos de backup ajuda a proteger seus dados contra perda ou exclusão não intencionais.

Correção

Para adicionar uma tabela do DynamoDB a AWS Backup um plano de backup, consulte Atribuição de recursos a um plano de backup no Guia do desenvolvedor.AWS Backup

[DynamoDB.5] As tabelas do DynamoDB devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-dynamodb-table` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se uma tabela do Amazon DynamoDB tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se a tabela não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a tabela não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma tabela do DynamoDB, consulte Como marcar recursos no DynamoDB no Amazon DynamoDB Developer Guide.

[DynamoDB.6] As tabelas do DynamoDB devem ter a proteção contra exclusão habilitada

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Proteger > Proteção de dados > Proteção contra exclusão de dados

Severidade: média

Tipo de recurso

AWS Config regra: **`dynamodb-table-deletion-protection-enabled`**

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma tabela do Amazon DynamoDB tem a proteção contra exclusão habilitada. O controle falhará se a tabela do DynamoDB não tiver a proteção contra exclusão habilitada.

É possível proteger uma tabela do DynamoDB contra exclusão acidental com a propriedade de proteção contra exclusão. Habilitar essa propriedade para tabelas ajuda a garantir que elas não sejam excluídas acidentalmente durante as operações regulares de gerenciamento de tabelas pelos administradores. Isso ajuda a evitar interrupções nas operações empresariais normais.

Correção

Para habilitar a proteção contra exclusão de uma tabela do DynamoDB, consulte Uso da proteção contra exclusão no Guia do desenvolvedor do Amazon DynamoDB.

[DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito

Requisitos relacionados: NIST.800-53.r5 AC-17, NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-13, Nist.800-53.r5 SC-23

Categoria: Proteger > Proteção de dados > Criptografia de dados em trânsito

Severidade: média

Tipo de recurso

AWS Config regra: **`dax-tls-endpoint-encryption`**

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um cluster do Amazon DynamoDB Accelerator (DAX) está criptografado em trânsito, com o tipo de criptografia de endpoint definido como TLS. O controle falhará se o cluster DAX não estiver criptografado em trânsito.

O HTTPS (TLS) pode ser usado para ajudar a impedir que possíveis invasores usem ataques semelhantes para espionar person-in-the-middle ou manipular o tráfego da rede. Você só deve permitir que conexões criptografadas via TLS acessem clusters DAX. No entanto, criptografar dados em trânsito pode afetar o desempenho. Você deve testar seu aplicativo com a criptografia ativada para entender o perfil de desempenho e o impacto do TLS.

Correção

Você não pode alterar a configuração de criptografia TLS depois de criar um cluster DAX. Para criptografar um cluster DAX existente, crie um novo cluster com a criptografia em trânsito ativada, transfira o tráfego do seu aplicativo para ele e, em seguida, exclua o cluster antigo. Para obter mais informações, consulte Usar a proteção contra exclusão no Guia do desenvolvedor do Amazon DynamoDB.

Amazon Elastic Container Registry

Esses controles estão relacionados aos recursos do Amazon ECR.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

Os repositórios privados do ECR devem ter a digitalização de imagens configurada

Requisitos relacionados: NIST.800-53.r5 CA-7

Categoria: Detectar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: alta

Tipo de recurso

Regra do AWS Config : `ecr-private-image-scanning-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um repositório privado do Amazon ECR tem a digitalização de imagens configurada. O controle falhará se o repositório ECR privado não estiver configurado para digitalização por push ou varredura contínua.

A verificação de imagens do ajuda a identificar vulnerabilidades de software nas imagens de seu contêiner. A configuração da digitalização de imagens em repositórios ECR adiciona uma camada de verificação da integridade e segurança das imagens que estão sendo armazenadas.

Correção

Para configurar a digitalização de imagens para um repositório ECR, consulte Digitalização de imagens no Guia do usuário do Amazon Elastic Container Registry.

[ECR.2] Os repositórios privados do ECR devem ter a imutabilidade da tag configurada

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Inventário

Severidade: média

Tipo de recurso

Regra do AWS Config : `ecr-private-tag-immutability-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um repositório ECR privado tem a imutabilidade de tags ativada. Esse controle falhará se um repositório ECR privado tiver a imutabilidade de tags desativada. Essa regra é aprovada se a imutabilidade da tag estiver ativada e tiver o valor `IMMUTABLE`.

O Amazon ECR Tag Immutability permite que os clientes confiem nas tags descritivas de uma imagem como um mecanismo confiável para rastrear e identificar imagens de forma exclusiva. Uma tag imutável é estática, o que significa que cada tag se refere a uma imagem exclusiva. Isso melhora a confiabilidade e a escalabilidade, pois o uso de uma tag estática sempre resultará na implantação da mesma imagem. Quando configurada, a imutabilidade das tags evita que elas sejam substituídas, o que reduz a superfície de ataque.

Correção

Para criar um repositório com tags imutáveis configuradas ou para atualizar as configurações de mutabilidade da tag de imagem para um repositório existente, consulte Mutabilidade da tag de imagem no Guia do usuário do Amazon Elastic Container Registry.

Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Configuração de recursos

Severidade: média

Tipo de recurso

Regra do AWS Config : `ecr-private-lifecycle-policy-configured`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um repositório do Amazon ECR tem pelo menos uma política de ciclo de vida configurada. Esse controle falhará se um repositório ECR não tiver nenhuma política de ciclo de vida configurada.

As políticas de ciclo de vida do Amazon ECR permitem que você especifique o gerenciamento do ciclo de vida das imagens em um repositório. Ao configurar as políticas de ciclo de vida, é possível automatizar a limpeza de imagens não usadas e a expiração das imagens com base na idade ou contagem. Automatizar essas tarefas pode ajudar você a evitar o uso involuntário de imagens desatualizadas em seu repositório.

Correção

Para configurar uma política de ciclo de vida, consulte Criar uma prévia da política de ciclo de vida no Guia do usuário do Amazon Elastic Container Registry.

[ECR.4] Os repositórios públicos do ECR devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ecr-publicrepository` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um repositório público do Amazon ECR tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o repositório público não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o repositório público não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um repositório público do ECR, consulte Como marcar um repositório público do Amazon ECR no Guia do usuário do Amazon Elastic Container Registry.

Controlador do Amazon ECS

Esses controles estão relacionados aos recursos da API de Gateway.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário.

Requisitos relacionados: NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-11, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-12

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: alta

Tipo de recurso

Regra do AWS Config : `ecs-task-definition-user-for-host-mode-check`

Tipo de programação: acionado por alterações

Parâmetros:

- `SkipInactiveTaskDefinitions`: `true` (não personalizável)

Esse controle verifica se uma definição de tarefa ativa do Amazon ECS com o modo de rede do host tem definições de contêiner de`privileged` ou `user`. O controle falha nas definições de tarefas que têm o modo de rede do host e as definições de contêiner de `privileged=false`, vazio e `user=root` ou vazio.

Esse controle avalia somente a revisão ativa mais recente de uma definição de tarefa do Amazon ECS.

O objetivo desse controle é garantir que o acesso seja definido intencionalmente quando você executa tarefas que usam o modo de rede do host. Se uma definição de tarefa tiver privilégios elevados, é porque você escolheu essa configuração. Esse controle verifica o escalonamento inesperado de privilégios quando uma definição de tarefa tem a rede de host ativada e você não escolhe privilégios elevados.

Correção

Para obter informações sobre como atualizar uma definição de tarefa, consulte Atualizar uma definição de tarefa no Guia do desenvolvedor do Amazon Elastic Container Service.

Quando você atualiza uma definição de tarefa, ela não atualiza as tarefas em execução que foram iniciadas a partir da definição de tarefa anterior. Para atualizar uma tarefa em execução, você deve reimplantar a tarefa com a nova definição de tarefa.

Os serviços do ECS não devem ter endereços IP públicos atribuídos a eles automaticamente

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Configuração de rede segura > Recursos não acessíveis ao público

Severidade: alta

Tipo de recurso

Regra AWS Config: `ecs-service-assign-public-ip-disabled` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

- `exemptEcsServiceArns` (não personalizável). O Security Hub não preenche esse parâmetro. Lista separada por vírgula de ARNs dos serviços do Amazon ECS que estão isentos dessa regra.

  Essa regra é `COMPLIANT` se um serviço do Amazon ECS tiver `AssignPublicIP` configurado como `ENABLED` e especificado nessa lista de parâmetros.

  Essa regra é `NON_COMPLIANT` se um serviço do Amazon ECS tiver `AssignPublicIP` configurado como `ENABLED` e especificado nessa lista de parâmetros.

Esse controle verifica se os serviços do Amazon ECS estão configurados para atribuir automaticamente endereços IP públicos. Esse controle falhará se `AssignPublicIP` for `ENABLED`. Esse controle será aprovado se `AssignPublicIP` for `DISABLED`.

Um endereço IP público é um endereço IPv4 que é acessível pela Internet. Se você iniciar suas instâncias do Amazon ECS com um endereço IP público, suas instâncias do Amazon ECS poderão ser acessadas pela internet. Os serviços do Amazon ECS não devem ser acessíveis ao público, pois isso pode permitir acesso não intencional aos seus servidores de aplicativos de contêineres.

Correção

Para desativar a atribuição automática de IP público, consulte Definir configurações de VPC e grupo de segurança para seu serviço no Guia do desenvolvedor do Amazon Elastic Container Service.

As definições de tarefas do ECS não devem compartilhar o namespace do processo do host

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Configuração de recursos

Severidade: alta

Tipo de recurso

AWS Config regra: ecs-task-definition-pid-mode-check

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se as definições de tarefas do Amazon ECS estão configuradas para compartilhar o namespace do processo de um host com seus contêineres. O controle falhará se a definição da tarefa compartilhar o namespace do processo do host com os contêineres em execução nele. Esse controle avalia somente a revisão ativa mais recente de uma definição de tarefa do Amazon ECS.

Um namespace de ID de processo (PID) fornece separação entre processos. Ele impede que os processos do sistema sejam visíveis e permite que os PIDs sejam reutilizados, incluindo o PID 1. Se o namespace PID do host for compartilhado com contêineres, isso permitirá que os contêineres vejam todos os processos no sistema host. Isso reduz o benefício do isolamento em nível de processo entre o host e os contêineres. Essas circunstâncias podem levar ao acesso não autorizado aos processos no próprio host, incluindo a capacidade de manipulá-los e encerrá-los. Os clientes não devem compartilhar o namespace do processo do host com os contêineres em execução nele.

Correção

Para configurar o `pidMode` na definição de uma tarefa, consulte Parâmetros de definição de tarefa no Guia do desenvolvedor do Amazon Elastic Container Service.

Os contêineres ECS devem ser executados sem privilégios

Requisitos relacionados: NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-11, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-12

Categoria: Proteger > Gerenciamento de acesso seguro > Recursos não acessíveis ao público

Severidade: alta

Tipo de recurso

Regra do AWS Config: ecs-containers-nonprivileged

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o parâmetro `privileged` na definição do contêiner das definições de tarefas do Amazon ECS está definido como `true`. O controle falhará se esse parâmetro for igual a `true`. Esse controle avalia somente a revisão ativa mais recente de uma definição de tarefa do Amazon ECS.

Recomendamos que você remova privilégios elevados de suas definições de tarefas do ECS. Quando esse parâmetro é verdadeiro, o contêiner recebe privilégios elevados na instância de contêiner host (semelhante ao usuário raiz).

Correção

Para configurar o `privileged` na definição de uma tarefa, consulte Parâmetros de definição de tarefa no Guia do desenvolvedor do Amazon Elastic Container Service.

Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz

Requisitos relacionados: NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-11, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-12

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: alta

Tipo de recurso

Regra do AWS Config: ecs-containers-readonly-access

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os contêineres do Amazon ECS estão limitados ao acesso somente de leitura aos sistemas de arquivos raiz montados. O controle falhará se o parâmetro `readonlyRootFilesystem` estiver definido como `false` ou se o parâmetro não existir na definição do contêiner dentro da definição da tarefa. Esse controle avalia somente a revisão ativa mais recente de uma definição de tarefa do Amazon ECS.

Ativar essa opção reduz os vetores de ataque à segurança, pois o sistema de arquivos da instância de contêiner não pode ser adulterado ou gravado, a menos que tenha permissões explícitas de leitura e gravação na pasta e nos diretórios do sistema de arquivos. Esse controle também segue o princípio do privilégio mínimo.

Correção

Limitar definições de contêiner para acesso somente leitura aos sistemas de arquivos raiz

1. Abra o console clássico do Amazon ECS em https://console.aws.amazon.com/ecs/.
2. No painel de navegação, escolha Task definitions (Definições de tarefa).
3. Selecione uma definição de tarefa que tenha definições de contêiner que precisam ser atualizadas. Para cada volume de dados, conclua as etapas a seguir.
   - No menu suspenso, escolha Criar nova revisão com JSON.
   - Adicione o parâmetro `readonlyRootFilesystem` e defina-o como `true` na definição do contêiner dentro da definição da tarefa.
   - Escolha Criar.

Os segredos não devem ser passados como variáveis de ambiente do contêiner

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Proteger > Desenvolvimento seguro > Credenciais sem codificação rígida

Severidade: alta

Tipo de recurso

Regra do AWS Config: ecs-no-environment-secrets

Tipo de programação: acionado por alterações

Parâmetros:

- secretKeys = `AWS_ACCESS_KEY_ID,AWS_SECRET_ACCESS_KEY,ECS_ENGINE_AUTH_DATA` (não personalizável)

Esse controle verifica se o valor-chave de qualquer variável no parâmetro `environment` das definições do contêiner inclui `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY` ou`ECS_ENGINE_AUTH_DATA`. Esse controle falhará se uma única variável de ambiente em qualquer definição de contêiner for igual a `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY` ou `ECS_ENGINE_AUTH_DATA`. Esse controle não abrange variáveis ambientais transmitidas de outros locais, como o Amazon S3. Esse controle avalia somente a revisão ativa mais recente de uma definição de tarefa do Amazon ECS.

AWS Systems Manager O Parameter Store pode ajudá-lo a melhorar a postura de segurança da sua organização. Recomendamos usar o Parameter Store para armazenar segredos e credenciais em vez de passá-los diretamente para suas instâncias de contêiner ou codificá-los em seu código.

Correção

Para criar parâmetros usando o SSM, consulte Criar parâmetros do Systems Manager no Guia do usuário do AWS Systems Manager . Para obter mais informações sobre a criação de uma definição de tarefa que especifica um segredo, consulte Especificar dados sigilosos usando segredos do Secrets Manager no Guia do desenvolvedor do Amazon Elastic Container Service.

As definições de tarefas do ECS devem ter uma configuração de registro em log

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: alta

Tipo de recurso

AWS Config regra: ecs-task-definition-log -configuração

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se a última definição de tarefa ativa do Amazon ECS tem uma configuração de registro em log especificada. O controle falhará se a definição da tarefa não tiver a propriedade `logConfiguration` definida ou se o valor para `logDriver` for nulo em pelo menos uma definição de contêiner.

O registro em log ajuda a manter a confiabilidade, a disponibilidade e a performance do Amazon ECS. A coleta de dados das definições de tarefas fornece visibilidade, o que pode ajudá-lo a depurar processos e encontrar a causa raiz dos erros. Se você estiver usando uma solução de registro em log que não precisa ser definida na definição de tarefas do ECS (como uma solução de registro em log de terceiros), é possível desabilitar esse controle depois de garantir que seus logs sejam capturados e entregues adequadamente.

Correção

Para definir uma configuração de log para suas definições de tarefas do Amazon ECS, consulte Especificar uma configuração de log na definição de tarefa no Guia do desenvolvedor do Amazon Elastic Container Service.

Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Detectar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: média

Tipo de recurso

Regra do AWS Config: `ecs-fargate-latest-platform-version`

Tipo de programação: acionado por alterações

Parâmetros:

- `latestLinuxVersion: 1.4.0` (não personalizável)
- `latestWindowsVersion: 1.0.0` (não personalizável)

O ECS.10 verifica se os serviços do Amazon ECS Fargate estão executando a versão da plataforma Fargate mais recente. Esse controle falhará se a versão da plataforma não for a mais recente.

AWS Fargate as versões de plataforma se referem a um ambiente de tempo de execução específico para a infraestrutura de tarefas do Fargate, que é uma combinação das versões de tempo de execução do kernel e do contêiner. Novas versões da plataforma são lançadas à medida que o ambiente de runtime evolui. Por exemplo, se houver atualizações do kernel ou do sistema operacional, novos recursos, correções de erros ou atualizações de segurança. As atualizações de segurança e patches são implantadas automaticamente nas tarefas do Fargate. Se for encontrado um problema de segurança que afete uma versão da plataforma, AWS corrija a versão da plataforma.

Correção

Para atualizar um serviço existente, incluindo sua versão da plataforma, consulte Atualizar um serviço no Guia do desenvolvedor do Amazon Elastic Container Service.

Os clusters do ECS devem usar Container Insights

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config: `ecs-container-insights-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os clusters do ECS usam o Container Insights. Esse controle falhará se o Container Insights não estiver configurado para um cluster.

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e o desempenho dos clusters do Amazon ECS. Use o CloudWatch Container Insights para coletar, agregar e resumir métricas e registros de seus aplicativos e microsserviços em contêineres. CloudWatch coleta automaticamente métricas para vários recursos, como CPU, memória,

disco e rede. O Container Insights também fornece informações de diagnóstico, como falhas de reinicialização de contêiner, para ajudar a isolar problemas e resolvê-los rapidamente. Você também pode definir CloudWatch alarmes nas métricas que o Container Insights coleta.

Correção

Para usar o Container Insights, consulte Atualização de um serviço no Guia CloudWatch do usuário da Amazon.

[ECS.13] Os serviços do ECS devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config: `tagged-ecs-service` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um serviço do Amazon ECS tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o serviço não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag

e falhará se o serviço não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um serviço do ECS, consulte Como marcar seus recursos do Amazon ECS no Guia do desenvolvedor do Amazon Elastic Container Service.

[ECS.14] Os clusters ECS devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config: `tagged-ecs-cluster` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um cluster do Amazon ECS tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o cluster não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o cluster não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive

AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um cluster do ECS, consulte Como marcar seus recursos do Amazon ECS no Guia do desenvolvedor do Amazon Elastic Container Service.

[ECS.15] As definições de tarefas do ECS devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config: `tagged-ecs-taskdefinition` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se uma definição de tarefa do Amazon ECS tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a definição da tarefa não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a definição da tarefa não estiver

marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com `aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma definição de tarefa do ECS, consulte Como marcar seus recursos do Amazon ECS no Amazon Elastic Container Service Developer Guide.

Amazon Elastic Compute Cloud - Compute

Esses controles estão relacionados aos recursos do Amazon EC2.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[PCI.EC2.1] Os instantâneos do Amazon EBS não devem ser restauráveis publicamente

Requisitos relacionados: PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/1.3.2,PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5

AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

Categoria: Proteger > Configuração de rede segura

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `ebs-snapshot-public-restorable-check`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se os instantâneos do Amazon Elastic Block Store não são públicos. O controle falhará se os instantâneos do Amazon EBS puderem ser restaurados por qualquer pessoa.

Os instantâneos do EBS são usados para fazer backup dos dados nos volumes do EBS no Amazon S3 em determinado momento. É possível usar os snapshots para restaurar estados anteriores de volumes do EBS. Raramente é aceitável compartilhar um snapshot com o público. Normalmente, a decisão de compartilhar um snapshot publicamente era tomada erroneamente ou sem uma compreensão completa das implicações. Essa verificação ajuda a garantir que todo esse compartilhamento tenha sido totalmente planejado e intencional.

Para tornar um instantâneo do EBS privado público, consulte Compartilhar um instantâneo no Guia do usuário do Amazon EC2 para instâncias Linux. Em Ações, modificar permissões, escolha Privado.

[EC2.2] O grupo de segurança padrão da VPC não deve permitir o tráfego de entrada e saída

Requisitos relacionados: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/2.1, CIS Foundations Benchmark v1.2.0/4.3, CIS Foundations Benchmark v1.4.0/5.3, CIS AWS Foundations Benchmark v3.0.0/5.4, NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), Nist.800-53.r5 SC-7, NIST.800-53.r5 AWS SC-7 (11), Nist.800-53.r5 SC-7 (16), NIST.800-53.R5 AWS SC-7 (21), NIST.800-53.r5 SC-7 (4), NISt.800-53.R5 SC-7 (5)

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso

Regra do AWS Config : `vpc-default-security-group-closed`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o grupo de segurança padrão de uma VPC não permite tráfego de entrada ou de saída. O controle falhará se o grupo de segurança permitir tráfego de entrada ou de saída.

As regras do grupo de segurança padrão permitem todo o tráfego de saída e entrada de interfaces de rede (e as instâncias associadas) que são atribuídas ao mesmo grupo de segurança. Recomendamos que você use a política de segurança padrão. Como o grupo de segurança padrão não pode ser excluído, altere a configuração das regras do grupo de segurança padrão para restringir o tráfego de entrada e saída. Isso evita o tráfego não intencional se o grupo de segurança padrão for acidentalmente configurado para recursos como as instâncias do EC2.

Correção

Para corrigir esse problema, comece criando novos grupos de segurança com privilégios mínimos. Para obter instruções, consulte Regras do grupo de segurança no Guia do usuário do Amazon VPC. Em seguida, atribua os novos grupos de segurança às suas instâncias do EC2. Para obter mais informações, consulte Alterar o grupo de segurança de uma instância no Manual do usuário do Amazon EC2 para instâncias do Linux.

Depois de atribuir os novos grupos de segurança aos seus recursos, remova todas as regras de entrada e saída dos grupos de segurança padrão. Para obter instruções, consulte Regras do grupo de segurança no Guia do usuário do Amazon VPC.

[EC2.3] Os volumes anexados do Amazon EBS devem ser criptografados em repouso.

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra do AWS Config : `encrypted-volumes`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os volumes do EBS em um estado anexado estão criptografados. Para passar nessa verificação, os volumes do EBS devem estar em uso e criptografados. Se o volume do EBS não estiver anexado, ele não estará sujeito a essa verificação.

Para obter uma camada adicional de segurança para os dados confidenciais nos volumes do EBS, habilite a criptografia em repouso do EBS. O Amazon EBS oferece uma solução simples de criptografia para os volumes do EBS que não exigem que você crie, mantenha e proteja sua própria infraestrutura de gerenciamento de chaves. Ele usa chaves mestras de cliente (CMKs) do ao criar volumes e instantâneos criptografados.

Para saber mais sobre a criptografia do Amazon EBS, consulte Criptografia do Amazon EBS no Guia do usuário do Amazon EC2 para instâncias do Linux.

Correção

Não há uma maneira direta de criptografar um volume ou instantâneo existente não criptografado. É possível criptografar um novo volume ou snapshot somente ao criá-lo.

Se você tiver habilitado a criptografia por padrão, o Amazon EBS criptografará o novo volume ou instantâneo resultante usando sua chave padrão para a criptografia do EBS. Mesmo se não tiver habilitado a criptografia por padrão, será possível habilitá-la ao criar um volume ou um snapshot individual. Em ambos os casos, é possível substituir a chave padrão para a criptografia do e escolher uma CMK simétrica gerenciada pelo cliente.

Para obter mais informações, consulte Criar um volume do Amazon EBS no Guia do usuário do Amazon EC2 para instâncias do Linux.

As instâncias EC2 interrompidas devem ser removidas após um período de tempo especificado

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Inventário

Severidade: média

Tipo de recurso

Regra do AWS Config : `ec2-stopped-instance`

Tipo de programação: Periódico

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`AllowedDays`	Número de dias em que a instância do EC2 pode ficar em um estado interrompido antes de gerar uma descoberta com falha.	Inteiro	1 para `365`	`30`

Esse controle verifica se uma instância do Amazon EC2 foi interrompida por mais do que o número de dias permitido. O controle falhará se uma instância do EC2 for interrompida por mais tempo do que o período máximo permitido. A menos que você forneça um valor de parâmetro personalizado para o período de tempo máximo permitido, o Security Hub usará um valor padrão de 30 dias.

Quando uma instância do EC2 não é executada por um período significativo de tempo, isso cria um risco de segurança porque a instância não está sendo mantida ativamente (analisada, corrigida, atualizada). Se for lançado posteriormente, a falta de manutenção adequada pode resultar em problemas inesperados em seu AWS ambiente. Para manter com segurança uma instância do EC2 ao longo do tempo em um estado inativo, inicie-a periodicamente para manutenção e depois interrompa-a após a manutenção. Idealmente, esse deve ser um processo automatizado.

Correção

Para encerrar uma instância inativa do Amazon EC2, consulte Encerrar uma instância no Guia do usuário do Amazon EC2 para instâncias do Linux.

[EC2.6] O registro de fluxo de VPC deve ser ativado em todas as VPCs

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/2.9, CIS Foundations Benchmark v1.4.0/3.9, CIS AWS Foundations Benchmark v3.0.0/3.7, PCI DSS v3.2.1/10.3.3, PCI DSS v3.2.1/10.3.4, AWS PCI DSS v3.2.1/10.3.6, Nist.800-53.r5 AC-5 4 (26), Nist.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NISt.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NISt.800-53.R5 CA-7, NISt.800-53.R5 SI-7 (8))

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `vpc-flow-logs-enabled`

Tipo de programação: Periódico

Parâmetros:

- `trafficType`: `REJECT` (não personalizável)

Verifica se os logs de fluxo do Amazon VPC estão localizados e habilitados para VPCs. O tipo de tráfego está definido como `Reject`.

É possível usar os logs de fluxo da VPC para capturar informações sobre tráfego IP de entrada e de saída nas interfaces de rede da VPC. Depois de criar um registro de fluxo, você pode visualizar e recuperar seus dados em CloudWatch Registros. Para reduzir custos, você também pode enviar seus logs de fluxo para o Amazon S3.

Recomendamos que você ative o registro de fluxo de rejeições de pacote para VPCs. Os registros de fluxo fornecem visibilidade sobre o tráfego de rede que percorre a VPC e podem detectar tráfego ou informações anormais durante fluxos de trabalho de segurança.

Por padrão, o registro inclui valores para os diferentes componentes do fluxo IP, incluindo a origem, o destino e o protocolo. Para obter mais informações e descrições dos campos de log, consulte VPC Flow Logs no Guia do usuário do Amazon VPC.

Correção

Para criar uma VPC, consulte Criar um fluxo de log no Guia do usuário do Amazon VPC. Depois de abrir o console do Amazon VPC, escolha Suas VPCs. Em Filter (Filtrar), escolha Reject (Rejeitar).

[EC2.7] A criptografia padrão do EBS deve estar ativada

Requisitos relacionados: CIS AWS Foundations Benchmark v1.4.0/2.2.1, CIS Foundations Benchmark v3.0.0/2.2.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 AWS CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28 (1), Nist.800-53.R5 SC-7 (10), Nist.800-53.R5 SI-7 (6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra do AWS Config : `ec2-ebs-encryption-by-default`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se a criptografia em nível de conta está habilitada por padrão para o Amazon Elastic Block Store (Amazon EBS). O controle falhará se a criptografia no nível da conta não estiver ativada.

Quando a criptografia está habilitada para sua conta, os volumes e as cópias de instantâneo do Amazon EBS são criptografados em repouso. Isso adiciona uma camada adicional de proteção aos dados. Para obter mais informações, consulte Encryption by default (Criptografia por padrão) no Manual do usuário do Amazon EC2 para instâncias do Linux.

Observe que os seguintes tipos de instância não oferecem suporte à criptografia: R1, C1 e M1.

Correção

Para obter mais informações, consulte a criptografia no Amazon EBS e Criptografia por padrão no Manual do usuário do Amazon EC2 para instâncias do Linux.

As instâncias do EC2 devem usar o Instance Metadata Service Version 2 (IMDSv2)

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/5.6, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Categoria: Proteger > Segurança de rede

Severidade: alta

Tipo de recurso

Regra do AWS Config : `ec2-imdsv2-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se a versão de metadados da instância do EC2 está configurada com o Instance Metadata Service versão 2 (IMDSv2). O controle é aprovado se `HttpTokens` estiver definido como necessário para o IMDSv2. O controle falha se `HttpTokens` estiver definido como `optional`.

Os metadados da instância são dados sobre sua instância que é possível usar para configurar ou gerenciar a instância em execução. O IMDS fornece acesso a credenciais temporárias e frequentemente alternadas. Essas credenciais eliminam a necessidade de codificar ou distribuir credenciais confidenciais às instâncias manual ou programaticamente. O IMDS é conectado localmente a cada instância do EC2. Ele é executado em um endereço IP especial de “link local” de 169.254.169.254. Esse endereço IP só pode ser acessado pelo software executado na instância.

A versão 2 do IMDS adiciona novas proteções para os seguintes tipos de vulnerabilidades. Essas vulnerabilidades podem ser usadas para tentar acessar o IMDS.

- Firewalls de aplicativos de sites abertos
- Proxies reversos abertos
- Vulnerabilidades de falsificação de solicitações do lado do servidor (SSRF)
- Firewalls Open Layer 3 e conversão de endereços de rede (NAT)

O Security Hub recomenda que você configure suas instâncias do EC2 com o IMDSv2.

Correção

Para configurar instâncias do EC2 com o IMDSv2, consulte Caminho recomendado para exigir o IMDSv2 no Guia do usuário do Amazon EC2 para instâncias Linux.

As instâncias do Amazon EC2 não devem ter um endereço IPv4 público

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso

Regra do AWS Config : `ec2-instance-no-public-ip`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se as instâncias do EC2 têm um endereço IP público. Essa regra será NON_COMPLIANT se o campo estiver presente no item de configuração da instância do . Esse controle se aplica somente aos endereços IPv4.

Um endereço IP público é um endereço IPv4 que é acessível pela Internet. Se você iniciar suas instâncias do Amazon ECS com um endereço IP público, suas instâncias do Amazon ECS poderão ser acessadas pela internet. Um endereço IPv4 privado é um endereço IP que não é acessível pela Internet. É possível usar endereços IPv4 privados para comunicação entre instâncias na mesma VPC.

Os endereços IPv6 são globalmente exclusivos e, portanto, acessíveis pela Internet. Por padrão, todas as sub-redes possuem o atributo de endereçamento IPv6 configurado como . Para obter mais informações sobre IPv6, consulte Endereçamento IP na sua VPC no Guia do usuário do Amazon VPC.

Se você tiver um caso de uso legítimo para manter instâncias do EC2 com endereços IP públicos, poderá suprimir as descobertas desse controle. Para obter mais informações sobre as opções de arquitetura front-end, consulte o blog AWS Architecture ou a série This Is My Architecture.

Correção

Como padrão, uma instância em uma VPC não padrão não recebe um endereço IPv4 público.

Quando você inicia uma instância em uma VPC padrão, atribuímos a ela um endereço IP público por padrão. Quando você executa uma instância do EC2 em uma VPC não padrão, a configuração da sub-rede determina se ela recebe um endereço IP público. A sub-rede tem um atributo para determinar se as novas instâncias do EC2 na sub-rede recebem um endereço IP público do grupo de endereços IPv4 públicos.

Você não pode associar ou desassociar manualmente um endereço IP público da instância. É possível controlar se sua instância recebe um endereço IP público fazendo o seguinte:

- Modificação do atributo de endereçamento IP público da sua sub-rede. Para obter mais informações, consulte Modificar o atributo de endereçamento IPv4 público para a sub-rede no Guia do usuário da Amazon VPC.

- Habilite ou desabilite o atributo de endereçamento de IP público durante a instância. Isso substitui o atributo de endereçamento de IP público da sub-rede. Para obter mais informações, consulte Atribuir um endereço IPv6 a uma instância, no Guia do usuário do Amazon EC2 para instâncias Linux.

Para obter mais informações, consulte Endereços IPv4 públicos e nomes de host DNS externos no Manual do usuário do Amazon EC2 para instâncias do Linux.

Caso contrário, associe um endereço IP elástico à sua instância depois que ela for iniciada para que ela possa ser acessada pela Internet. É possível desassociar um endereço IP elástico de uma instância ou interface de rede a qualquer momento. Conclua as etapas em Desassociar um endereço IP elástico no Guia do usuário do Amazon EC2 para instâncias do Linux para desassociar o EIP.

O Amazon EC2 deve ser configurado para usar endpoints da VPC criados para o serviço Amazon EC2

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso

Regra do AWS Config : `service-vpc-endpoint-enabled`

Tipo de programação: Periódico

Parâmetros:

- `serviceName`: `ec2` (não personalizável)

Esse controle verifica se um endpoint de serviço para o Amazon EC2 foi criado para cada VPC. O controle falhará se uma VPC não tiver um endpoint da VPC criado para o serviço Amazon EC2.

Esse controle avalia os recursos em uma única conta. Ela não pode descrever recursos que estão fora da conta. Como AWS Config o Security Hub não realiza verificações entre contas, você verá

`FAILED` descobertas de VPCs que são compartilhadas entre contas. O Security Hub recomenda que você suprima essas descobertas `FAILED`.

É possível melhorar a postura de segurança da sua VPC configurando o Amazon EC2 para usar um VPC endpoint de interface. Os endpoints de interface são alimentados por AWS PrivateLink, uma tecnologia que permite acessar as operações de API do Amazon EC2 de forma privada. O PrivateLink restringe todo o tráfego de rede entre sua VPC e o Amazon ECR para a rede da Amazon. Como os endpoints são suportados somente na mesma região, não é possível criar um endpoint entre uma VPC e um serviço em uma região diferente. Isso evita chamadas não intencionais da API do Amazon EC2 para outras regiões.

Para saber mais sobre como criar endpoints da VPC para o Amazon EC2, consulte Amazon EC2 e endpoints da VPC de interface no Guia do usuário do Amazon EC2 para instâncias Linux.

Correção

Para criar um endpoint de interface para o Amazon EC2 a partir do console Amazon VPC, consulte Criar um endpoint da VPC no Guia do AWS PrivateLink . Em Service Name (Nome do serviço), selecione com.amazonaws.***região***.lambda.

É possível associar uma política ao seu VPC endpoint para controlar o acesso à API do Amazon EC2. Para obter instruções sobre como criar uma política de endpoint da VPC, consulte Criar uma política de endpoint no Guia do usuário do Amazon EC2 para instâncias Linux.

[PCI.EC2.4] Os EIPs do EC2 não utilizados devem ser removidos

Requisitos relacionados: PCI DSS v3.2.1/8.2.1, NIST.800-53.r5 SA-3

Categoria: Proteger > Configuração de rede segura

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `eip-attached`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os endereços IP elásticos que estão alocados a uma VPC estão anexados a instâncias do ou a interfaces de rede elástica (ENIs) em uso.

Uma falha na descoberta indica que é possível ter EIPs do EC2 não utilizados

Isso ajudará a manter um inventário preciso de ativos de EIPs no CDE.

Para saber mais, consulte Endereços IP elásticos no Manual do usuário do Amazon EC2 para instâncias do Linux.

[EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/4.1, PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/2.2.2, NIST.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), NIST.800-53.r5 CM-7, SCIst.800-53.r5 Nist.800-53.r5 SC-7 (11), Nist.800-53.R5 SC-7 (16), Nist.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (4), Nist.800-53.R5 SC-7 (5)

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso

Regra do AWS Config : `restricted-ssh`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um grupo de segurança do Amazon EC2 permite a entrada de 0.0.0/0 ou ::/0 na porta 22. O controle falhará se o grupo de segurança permitir a entrada de 0.0.0/0 ou ::/0 na porta 22.

Os grupos de segurança fornecem filtragem stateful de tráfego de rede de entrada e saída aos recursos da AWS . Recomendamos que nenhum grupo de segurança permita o acesso de entrada irrestrito à porta 22. A remoção de conectividade sem restrições aos serviços de console remotos, como SSH, reduz a exposição do servidor ao risco.

Correção

Para proibir a entrada na porta 22, remova a regra que permite esse acesso para cada grupo de segurança associado a uma VPC. Para obter instruções, consulte Atualizar as regras do grupo de segurança no Guia do usuário do Amazon EC2 para instâncias Linux. Depois de selecionar um

grupo de segurança no console do Amazon EC2, escolha Ações, Editar regras de entrada. Remova a regra que permite o acesso à porta 22.

[EC2.14] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 3389

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/4.2

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso

AWS Config regra: **`restricted-common-ports`**(a regra criada é`restricted-rdp`)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um grupo de segurança do Amazon EC2 permite a entrada de 0.0.0/0 ou ::/0 na porta 3389. O controle falhará se o grupo de segurança permitir a entrada de 0.0.0/0 ou ::/0 na porta 3389.

Os grupos de segurança fornecem filtragem stateful de tráfego de rede de entrada e saída aos recursos da AWS . Recomendamos que nenhum grupo de segurança de entrada para permitir acesso irrestrito a porta 3389. A remoção de conectividade sem restrições aos serviços de console remotos, como RDP, reduz a exposição do servidor ao risco.

Correção

Para proibir a entrada na porta 22, remova a regra que permite esse acesso para cada grupo de segurança associado a uma VPC. Para obter instruções, consulte Regras do grupo de segurança no Guia do usuário do Amazon VPC. Depois de selecionar um grupo de segurança no console do Amazon VPC, escolha Ações, editar regras de entrada. Remova a regra que permite o acesso à porta 22.

As sub-redes do Amazon EC2 não devem atribuir automaticamente endereços IP públicos

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3),

NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Segurança de rede

Severidade: média

Tipo de recurso

Regra do AWS Config : `subnet-auto-assign-public-ip-disabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se a atribuição de IPs públicos nas sub-redes da Amazon Virtual Private Cloud (Amazon VPC) tem `MapPublicIpOnLaunch` definido como `FALSE`. O controle é aprovado se o sinalizador estiver definido como `FALSE`.

Todas as sub-redes têm um atributo que determina se uma interface de rede criada na sub-rede recebe automaticamente um endereço público IPv4 (também referido como um endereço IP público neste tópico). As instâncias que são executadas em sub-redes com esse atributo ativado têm um endereço IP público atribuído à interface de rede primária.

Correção

Para configurar uma sub-rede para não atribuir endereços IP públicos, consulte Modificar o atributo de endereçamento IPv4 público para a sub-rede no Guia do usuário do Amazon VPC. Desmarque a caixa de seleção Ativar atribuição automática de endereço IPv4 público.

As listas de controle de acesso à rede não utilizadas devem ser removidas

Requisitos relacionados: NIST.800-53.r5 CA-7

Categoria: Proteger > Segurança de rede

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `vpc-network-acl-unused-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se há listas de controle de acesso (ACLs) à rede não utilizadas.

O controle verifica a configuração do recurso `AWS::EC2::NetworkAcl` e determina as relações da ACL de rede.

Se o único relacionamento for a VPC da ACL de rede, o controle falhará.

Se outros relacionamentos estiverem listados, o controle será aprovado.

Correção

Para obter instruções sobre como excluir uma ACL de rede não utilizada, consulte Excluir uma ACL de rede no Guia do usuário do Amazon VPC. Não é possível excluir a ACL de rede padrão ou uma ACL associada a sub-redes.

As instâncias do Amazon EC2 não devem usar vários ENIs

Requisitos relacionados: NIST.800-53.r5 CA-7

Categoria: Proteger > Segurança de rede

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `ec2-instance-multiple-eni-check`

Tipo de programação: acionado por alterações

Parâmetros:

- `Adapterids`: uma lista de IDs de interface de rede que estão vinculadas às instâncias do EC2 (não personalizável)

Esse controle verifica se uma instância do EC2 usa várias interfaces de rede elásticas (ENI) ou Elastic Fabric Adapters (EFAs). Esse controle passa se um único adaptador de rede for usado. O controle inclui uma lista de parâmetros opcional para identificar os ENIs permitidos. Esse controle

também falhará se uma instância do EC2 que pertence a um cluster do Amazon EKS usar mais de uma ENI. Se suas instâncias do EC2 precisarem ter várias ENIs como parte de um cluster do Amazon EKS, será possível suprimir essas descobertas de controle.

Vários ENIs podem causar instâncias com hospedagem dupla, ou seja, instâncias que têm várias sub-redes. Isso pode aumentar a complexidade da segurança da rede e introduzir caminhos e acessos de rede não intencionais.

Correção

Para separar uma interface de rede de uma instância do EC2, consulte Separar uma interface de rede de uma instância no Guia do usuário do Amazon EC2 para instâncias Linux.

Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Configuração de rede segura > Configuração do grupo de segurança

Severidade: alta

Tipo de recurso

Regra do AWS Config : `vpc-sg-open-only-to-authorized-ports`

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`authorizedTcpPorts`	Lista de portas TCP autorizadas	IntegerList (máximo de 32 itens)	1 para 65535	`[80,443]`

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`authorizedUdpPorts`	Lista de portas UDP autorizadas	IntegerList (máximo de 32 itens)	1 para 65535	Nenhum valor padrão

Esse controle verifica se um grupo de segurança do Amazon EC2 permite tráfego de entrada irrestrito em portas não autorizadas. O status do controle é determinado da forma a seguir:

- Se você usar o valor padrão para `authorizedTcpPorts`, o controle falhará se o grupo de segurança permitir tráfego de entrada irrestrito em qualquer porta que não seja as portas 80 e 443.
- Se você fornecer valores personalizados para `authorizedTcpPorts` ou `authorizedUdpPorts`, o controle falhará se o grupo de segurança permitir tráfego de entrada irrestrito em qualquer porta não listada.
- Se nenhum parâmetro for usado, o controle falhará em qualquer grupo de segurança que tenha uma regra de tráfego de entrada irrestrita.

Os grupos de segurança fornecem filtragem stateful de tráfego de rede de entrada e saída aos recursos da AWS. As regras do grupo de segurança devem seguir o princípio do acesso de privilégio mínimo. O acesso irrestrito (endereço IP com sufixo /0) aumenta a oportunidade de atividades maliciosas, como invasões, denial-of-service ataques e perda de dados. A menos que uma porta seja especificamente permitida, a porta deve negar acesso irrestrito.

Correção

Para modificar um grupo de segurança, consulte Trabalho com grupos de segurança no Guia do usuário da Amazon VPC.

Grupos de segurança não devem permitir acesso irrestrito a portas com alto risco

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Acesso restrito à rede

Severidade: crítica

Tipo de recurso

AWS Config regra: **`restricted-common-ports`**(a regra criada é`vpc-sg-restricted-common-ports`)

Tipo de programação: acionado por alterações

Parâmetros: `"blockedPorts": "20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,560` (não personalizável)

Esse controle verifica se o tráfego de entrada irrestrito para um grupo de segurança do Amazon EC2 está acessível às portas especificadas que são consideradas de alto risco. Esse controle falhará se alguma das regras em um grupo de segurança permitir tráfego de entrada de '0.0.0.0/0' ou '::/0' nessas portas.

Os grupos de segurança fornecem filtragem stateful de tráfego de rede de entrada e saída aos recursos da AWS . O acesso irrestrito (0.0.0.0/0) aumenta as oportunidades de atividades maliciosas, como invasões, denial-of-service ataques e perda de dados. Nenhum grupo de segurança deve permitir acesso irrestrito de entrada às seguintes portas:

- 20, 21 (FTP)
- 22 (SSH)
- 23 (Telnet)
- 25 (SMTP)
- 110 (POP 3)
- 135 (RPM)
- 143 (IMAPA)
- 445 (CIFS)
- 1433 (MS SQL)
- 3000 (estruturas de desenvolvimento web Go, Node.js e Ruby)
- 3306 (MySQL)

- 3389 (RDP)
- 4333 (ahsp)
- 5000 (estruturas de desenvolvimento web em Python)
- 5432 (PostgreSQL)
- 500 (fcp-addr-srvr1)
- 5601 (Painéis) OpenSearch
- 8080 (proxy)
- 8088 (porta HTTP antiga)
- 8888 (porta HTTP alternativa)
- 9200 ou 9300 () OpenSearch

Correção

Para excluir regras de um grupo de segurança, consulte Excluir regras de um grupo de segurança no Guia do usuário do Amazon EC2 para instâncias Linux.

[EC2.20] Ambos os túneis VPN para uma conexão VPN Site-to-Site devem estar ativos AWS

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Resiliência > Recuperação > Alta disponibilidade

Severidade: média

Tipo de recurso`AWS::EC2::VPNConnection`

Regra do AWS Config : `vpc-vpn-2-tunnels-up`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Um túnel VPN é um link criptografado em que os dados podem passar da rede do cliente para ou de AWS dentro de uma AWS conexão VPN Site-to-Site. Cada conexão VPN inclui dois túneis VPN que podem ser usados simultaneamente para alta disponibilidade. Garantir que os dois túneis

VPN estejam prontos para uma conexão VPN é importante para confirmar uma conexão segura e altamente disponível entre uma AWS VPC e sua rede remota.

Esse controle verifica se os dois túneis VPN fornecidos pela VPN AWS Site-to-Site estão no status UP. O controle falhará se um ou ambos os túneis estiverem no status DOWN.

Correção

Para modificar as opções de túnel VPN, consulte Modificação das opções de túnel VPN Site-to-Site no Guia do usuário da AWS VPN Site-to-Site.

As ACLs de rede não devem permitir a entrada de 0.0.0.0/0 para a porta 22 ou porta 3389

Requisitos relacionados: CIS AWS Foundations Benchmark v1.4.0/5.1, CIS Foundations Benchmark v3.0.0/5.1, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 AWS CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-7 Nist.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (5)

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso`AWS::EC2::NetworkAcl`

Regra do AWS Config : `nacl-no-unrestricted-ssh-rdp`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma lista de controle de acesso à rede (NACL) permite acesso irrestrito às portas TCP padrão para tráfego de entrada SSH/RDP. A regra falhará se uma entrada NACL permitir um bloco CIDR de origem de '0.0.0.0/0' ou ': :/0' para as portas TCP 22 ou 3389.

O acesso às portas de administração remota do servidor, como a porta 22 (SSH) e a porta 3389 (RDP), não deve ser acessível ao público, pois isso pode permitir acesso não intencional aos recursos em sua VPC.

Correção

Para obter mais informações, consulte ACLs da rede no Guia do usuário do Amazon VPC

[PCI.EC2.3] Os grupos de segurança do Amazon EC2 devem ser removidos

> **Important**
>
> RETIRADO DE PADRÕES ESPECÍFICOS — O Security Hub removeu esse controle em 20 de setembro de 2023 do padrão AWS Foundational Security Best Practices e do NIST SP 800-53 Rev. 5. Esse controle ainda faz parte do Service-Managed Standard:. AWS Control Tower Esse controle da produz uma descoberta aprovada se os grupos de segurança estiverem conectados a instâncias do EC2 ou a uma interface de rede elástica. Entretanto, para determinados casos de uso, grupos de segurança independentes não representam um risco de segurança. É possível usar outros controles do EC2, como EC2.2, EC2.13, EC2.14, EC2.18 e EC2.19, para monitorar seus grupos de segurança.

Categoria: Identificar > Inventário

Severidade: média

Tipo de recurso

Regra do AWS Config : `ec2-security-group-attached-to-eni-periodic`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse AWS controle verifica se os grupos de segurança estão vinculados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou a uma interface de rede elástica. A regra retornará NON_COMPLIANT se o grupo de segurança não estiver associado a uma instância do Amazon EC2 ou a uma interface de rede elástica.

Correção

Para criar, atribuir e excluir grupos de segurança, consulte Grupos de segurança no guia do usuário do Amazon EC2.

Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC

Requisitos relacionados: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso`AWS::EC2::TransitGateway`

Regra do AWS Config : `ec2-transit-gateway-auto-vpc-attach-disabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os gateways de trânsito do EC2 estão aceitando automaticamente anexos de VPC compartilhados. Esse controle falha em um gateway de trânsito que aceita automaticamente solicitações compartilhadas de anexos de VPC.

A ativação de `AutoAcceptSharedAttachments` configura um gateway de trânsito para aceitar automaticamente qualquer solicitação de anexo de VPC entre contas sem verificar a solicitação ou a conta da qual o anexo é originário. Para seguir as melhores práticas de autorização e autenticação, recomendamos desativar esse atributo para garantir que somente solicitações autorizadas de anexos de VPC sejam aceitas.

Correção

Para modificar um gateway de trânsito, consulte Modificar um gateway de trânsito no Guia do desenvolvedor do Amazon VPC.

Os tipos de instância paravirtual do Amazon EC2 não devem ser usados

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Detectar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: média

Tipo de recurso`AWS::EC2::Instance`

Regra do AWS Config : `ec2-paravirtual-instance-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Verifica se o tipo de virtualização de uma instância do Amazon EC2 é paravirtual. O controle falhará se o `virtualizationType` da instância do EC2 estiver definida como `paravirtual`.

As Imagens de máquina da Amazon em Linux usam um dos dois tipos de virtualização: paravirtual (PV) ou máquina virtual de hardware (HVM). As diferenças principais entre as AMIs PV e HVM são a maneira como elas inicializam e se podem aproveitar extensões especiais de hardware (CPU, rede e armazenamento) para melhor performance.

Historicamente, os guests PV têm melhor performance que os guests HVM em muitos casos, mas devido a aprimoramentos na virtualização de HVM e disponibilidade de drivers PV para AMIs HVM, isso não é mais verdadeiro. Para obter mais informações, consulte Tipos de virtualização da AMI em Linux no Guia do usuário do Amazon EC2 para instâncias do Linux.

Correção

Para atualizar uma instância do EC2 para um novo tipo de instância, consulte Alterar o tipo de instância no Guia do usuário do Amazon EC2 para instâncias Linux.

Os modelos de lançamento do Amazon EC2 não devem atribuir IPs públicos às interfaces de rede

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Configuração de rede segura > Recursos não acessíveis ao público

Severidade: alta

Tipo de recurso`AWS::EC2::LaunchTemplate`

Regra do AWS Config : `ec2-launch-template-public-ip-disabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os modelos de execução do Amazon EC2 estão configurados para atribuir endereços IP públicos às interfaces de rede após o lançamento. O controle falhará se um modelo de

execução do EC2 estiver configurado para atribuir um endereço IP público às interfaces de rede ou se houver pelo menos uma interface de rede que tenha um endereço IP público.

Um endereço IP público é um endereço IPv4 que é acessível pela Internet. Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a essas interfaces de rede poderão ser acessados pela Internet. Os recursos do EC2 não devem ser acessíveis ao público, pois isso pode permitir acesso não intencional às suas workloads.

Correção

Para atualizar um modelo de execução do EC2, consulte Alterar as configurações de interface de rede padrão no Guia do usuário do Amazon EC2 Auto Scaling.

[EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup

Categoria: Recuperação > Resiliência > Backups ativados

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Severidade: baixa

Tipo de recurso

AWS Config regra: **`ebs-resources-protected-by-backup-plan`**

Tipo de programação: Periódico

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`backupVaultLockCheck`	O controle produz uma `PASSED` descoberta se o parâmetro estiver definido como `true` e o recurso usar o AWS Backup Vault Lock.	Booleano	`true` ou `false`	Nenhum valor padrão

Esse controle avalia se um volume do Amazon EBS no estado `in-use` está coberto por um plano de backup. O controle falhará se um volume do EBS não estiver coberto por um plano de backup. Se você definir o `backupVaultLockCheck` parâmetro igual `atrue`, o controle passará somente se o volume do EBS for copiado em um cofre AWS Backup bloqueado.

Os backups ajudam você a se recuperar mais rapidamente de um incidente de segurança. Eles também fortalecem a resiliência de seus sistemas. Incluir os volumes do Amazon EBS em seus planos de backup ajuda a proteger seus dados contra perda ou exclusão não intencionais.

Correção

Para adicionar um volume do Amazon EBS a um plano de AWS Backup backup, consulte Atribuição de recursos a um plano de backup no Guia do AWS Backup desenvolvedor.

[EC2.33] Os anexos do gateway de trânsito EC2 devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-transitgatewayattachment` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um anexo do gateway de trânsito do Amazon EC2 tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o anexo do gateway de trânsito não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o anexo do gateway de trânsito não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para [que serve o ABAC](#)? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como [marcar seus AWS recursos](#) no. Referência geral da AWS

Correção

Para adicionar tags a um anexo do gateway de trânsito do EC2, consulte [Marcar seus recursos do Amazon EC2](#) no Guia do usuário do Amazon EC2 para instâncias Linux.

[EC2.34] As tabelas de rotas do gateway de trânsito EC2 devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-transitgatewayroutetable` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se uma tabela de rotas do gateway de trânsito do Amazon EC2 tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se a tabela de rotas do gateway de trânsito não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a tabela de rotas do gateway de trânsito não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM.

Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma tabela de rotas do gateway de trânsito do EC2, consulte Marcar seus recursos do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias Linux.

[EC2.35] As interfaces de rede EC2 devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-networkinterface` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter.	StringList	Lista de tags que atendem	Nenhum valor padrão

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	Chaves de tag fazem distinção entre maiúsculas e minúsculas.		aos AWS requisitos	

Esse controle verifica se uma interface de rede do Amazon EC2 tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se a interface de rede não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a interface de rede não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma interface de rede do EC2, consulte Marcar seus recursos do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias Linux.

[EC2.36] Os gateways de clientes do EC2 devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-customergateway` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um gateway de cliente do Amazon EC2 tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o gateway do cliente não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o gateway do cliente não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um gateway de cliente do EC2, consulte Marcar seus recursos do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias Linux.

[EC2.37] Os endereços IP elásticos do EC2 devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-eip` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um endereço IP elástico do Amazon EC2 tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o endereço IP elástico não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o endereço IP elástico não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive

AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um endereço IP elástico do EC2, consulte Marcar seus recursos do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias Linux.

[EC2.38] As instâncias do EC2 devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-instance` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se uma instância do Amazon EC2 tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se a instância não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave

de tag e falhará se a instância não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma instância do EC2, consulte Marcar seus recursos do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias Linux.

[EC2.39] Os gateways de internet EC2 devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-internetgateway` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um gateway de internet do Amazon EC2 tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o gateway da Internet não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle verificará apenas a existência de uma chave de tag e falhará se o gateway da Internet não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive

AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um gateway de internet EC2, consulte Marcar seus recursos do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias Linux.

[EC2.40] Os gateways NAT EC2 devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-natgateway` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um gateway de tradução de endereços de rede (NAT) do Amazon EC2 tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o gateway NAT não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o gateway NAT não estiver marcado com

nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com `aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um gateway NAT do EC2, consulte Marcar seus recursos do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias Linux.

[EC2.41] As ACLs de rede EC2 devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-networkacl` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se uma lista de controle de acesso à rede do Amazon EC2 (Network ACL) tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se a rede ACL não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle somente verificará a existência de uma chave de tag e falhará se a ACL da rede não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive

AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma ACL de rede EC2, consulte Marcar seus recursos do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias Linux.

[EC2.42] As tabelas de rotas do EC2 devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-routetable` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se uma tabela de rotas do Amazon EC2 tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se a tabela de rotas não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a tabela de rotas não estiver marcada com

nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com `aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma tabela de rotas do EC2, consulte Marcar seus recursos do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias Linux.

[EC2.43] Grupos de segurança do EC2 devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-securitygroup` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um grupo de segurança do Amazon EC2 tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o grupo de segurança não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o grupo de segurança não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive

AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um grupo de segurança do EC2, consulte Marcar seus recursos do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias Linux.

[EC2.44] As sub-redes do EC2 devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-subnet` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se uma sub-rede do Amazon EC2 tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se a sub-rede não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o

parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a sub-rede não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para [que serve o ABAC]? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como [marcar seus AWS recursos] no. Referência geral da AWS

Correção

Para adicionar tags a uma sub-rede do EC2, consulte [Marcar seus recursos do Amazon EC2] no Guia do usuário do Amazon EC2 para instâncias Linux.

[EC2.45] Os volumes do EC2 devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-subnet` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um volume do Amazon EC2 tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o volume não tiver nenhuma chave de tag ou se não tiver todas as teclas especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o volume não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive

AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um volume do EC2, consulte Marcar seus recursos do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias Linux.

[EC2.46] Amazon VPCs devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-vpc` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se uma Amazon Virtual Private Cloud (Amazon VPC) tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se a Amazon VPC não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro. `requiredTagKeys` Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a Amazon VPC não estiver marcada com nenhuma

chave. As tags do sistema, que são aplicadas automaticamente e começam com `aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma VPC, consulte Marcar seus recursos do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias Linux.

[EC2.47] Os serviços de endpoint da Amazon VPC devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-vpcendpointservice` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um serviço de endpoint da Amazon VPC tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o serviço de endpoint não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o serviço de endpoint não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive

AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um serviço de endpoint da Amazon VPC, consulte Gerenciar tags na seção Configurar um serviço de endpoint do Guia.AWS PrivateLink

[EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-flowlog` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um log de fluxo da Amazon VPC tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o registro de fluxo não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle

só verificará a existência de uma chave de tag e falhará se o log de fluxo não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com `aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags podem ser acessadas por muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um log de fluxo da Amazon VPC, consulte Marcar um log de fluxo no Guia do usuário da Amazon VPC.

[EC2.49] As conexões de emparelhamento da Amazon VPC devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-vpcpeeringconnection` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se uma conexão de emparelhamento da Amazon VPC tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se a conexão de emparelhamento não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a conexão de peering não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma conexão de emparelhamento do Amazon VPC, consulte Marcar seus recursos do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias Linux.

[EC2.50] Os gateways de VPN EC2 devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-vpngateway` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um gateway VPN do Amazon EC2 tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o gateway VPN não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle verificará apenas a existência de uma chave de tag e falhará se o gateway de VPN não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para [que serve o ABAC](#)? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como [marcar seus AWS recursos](#) no. Referência geral da AWS

Correção

Para adicionar tags a um gateway de VPN EC2, consulte [Marcar seus recursos do Amazon EC2](#) no Guia do usuário do Amazon EC2 para instâncias Linux.

[EC2.51] Os endpoints da Client VPN do EC2 devem ter o registro em log de conexão do cliente habilitado

Requisitos relacionados: CIS Foundations Benchmark v1.2.0/2.1, CIS Foundations Benchmark v1.4.0/3.1, NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9),

NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-14(1), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8), NIST.800-53.r5 SA-8(22)

Categoria: Identificar > Registro em log

Severidade: baixa

Tipo de recurso

AWS Config regra: **`ec2-client-vpn-connection-log-enabled`**

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um AWS Client VPN endpoint tem o registro de conexão do cliente ativado. O controle falhará se o endpoint não tiver o registro em log de conexão do cliente habilitado.

Os endpoints do Client VPN permitem que clientes remotos se conectem com segurança aos recursos em uma nuvem privada virtual (VPC) na AWS. Os registros em log de conexão permitem que você acompanhe a atividade do usuário no endpoint da VPN e forneça visibilidade. Ao habilitar o registro em log de conexão, é possível especificar o nome de um stream de logs no grupo de logs. Se você não especificar um fluxo de logs, o serviço do Client VPN criará um para você.

Correção

Para habilitar o registro em log de conexão, consulte Habilitar o registro em log de conexão para um endpoint do Client VPN existente no Manual do administrador do AWS Client VPN .

[EC2.52] Os gateways de trânsito do EC2 devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-ec2-transitgateway` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um gateway de trânsito do Amazon EC2 tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o gateway de trânsito não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o gateway de trânsito não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS

Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um gateway de trânsito do EC2, consulte Marcar seus recursos do Amazon EC2 no Guia do usuário do Amazon EC2 para instâncias Linux.

[EC2.53] Os grupos de segurança do EC2 não devem permitir a entrada de 0.0.0.0/0 nas portas de administração remota do servidor

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/5.2

Categoria: Proteger > Configuração de rede segura > Configuração do grupo de segurança

Severidade: alta

Tipo de recurso

Regra do AWS Config : `vpc-sg-port-restriction-check`

Tipo de programação: Periódico

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`ipType`	A versão IP	String	Não personalizável	`IPv4`
`restrictPorts`	Lista de portas que devem rejeitar o tráfego de entrada	IntegerList	Não personalizável	`22,3389`

Esse controle verifica se um grupo de segurança do Amazon EC2 permite a entrada de 0.0.0.0/0 nas portas de administração remota do servidor (portas 22 e 3389). O controle falhará se o grupo de segurança permitir a entrada de 0.0.0.0/0 para a porta 22 ou 3389.

Os grupos de segurança fornecem filtragem com estado do tráfego de entrada e saída da rede para os recursos. AWS Recomendamos que nenhum grupo de segurança permita acesso irrestrito às portas de administração do servidor remoto, como SSH na porta 22 e RDP na porta 3389, usando os protocolos TDP (6), UDP (17) ou ALL (-1). Permitir o acesso público a essas portas aumenta a superfície de ataque dos recursos e o risco de comprometimento dos recursos.

Correção

Para atualizar uma regra de grupo de segurança do EC2 para proibir o tráfego de entrada nas portas especificadas, consulte Atualizar regras do grupo de segurança no Guia do usuário do Amazon EC2 para instâncias Linux. Depois de selecionar um grupo de segurança no console do Amazon EC2, escolha Ações, Editar regras de entrada. Remova a regra que permite o acesso à porta 22 ou à porta 3389.

[EC2.54] Os grupos de segurança do EC2 não devem permitir a entrada de: :/0 nas portas de administração do servidor remoto

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/5.3

Categoria: Proteger > Configuração de rede segura > Configuração do grupo de segurança

Severidade: alta

Tipo de recurso

Regra do AWS Config : `vpc-sg-port-restriction-check`

Tipo de programação: Periódico

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`ipType`	A versão IP	String	Não personalizável	`IPv6`
`restrictPorts`	Lista de portas que devem rejeitar o tráfego de entrada	IntegerList	Não personalizável	`22,3389`

Esse controle verifica se um grupo de segurança do Amazon EC2 permite a entrada de: :/0 nas portas de administração remota do servidor (portas 22 e 3389). O controle falhará se o grupo de segurança permitir a entrada de: :/0 para a porta 22 ou 3389.

Os grupos de segurança fornecem filtragem com estado do tráfego de entrada e saída da rede para os recursos. AWS Recomendamos que nenhum grupo de segurança permita acesso irrestrito às portas de administração do servidor remoto, como SSH na porta 22 e RDP na porta 3389, usando os protocolos TDP (6), UDP (17) ou ALL (-1). Permitir o acesso público a essas portas aumenta a superfície de ataque dos recursos e o risco de comprometimento dos recursos.

Correção

Para atualizar uma regra de grupo de segurança do EC2 para proibir o tráfego de entrada nas portas especificadas, consulte Atualizar regras do grupo de segurança no Guia do usuário do Amazon EC2 para instâncias Linux. Depois de selecionar um grupo de segurança no console do Amazon EC2, escolha Ações, Editar regras de entrada. Remova a regra que permite o acesso à porta 22 ou à porta 3389.

Grupo do Amazon EC2 Auto Scaling

Esses controles estão relacionados aos recursos do Amazon EC2 Auto Scaling.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[AutoScaling.1] Grupos de Auto Scaling associados a um balanceador de carga devem usar verificações de integridade do ELB

Requisitos relacionados: PCI DSS v3.2.1/2.2, NIST.800-53.r5 CA-7, NIST.800-53.r5 CP-2(2), NIST.800-53.r5 SI-2

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `autoscaling-group-elb-healthcheck-required`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um grupo do Amazon EC2 Auto Scaling associado a um balanceador de carga usa as verificações de saúde do Elastic Load Balancing (ELB). O controle falhará se o grupo Auto Scaling não usar as verificações de integridade do ELB.

As verificações de integridade do ELB ajudam a garantir que um grupo do Auto Scaling possa determinar a integridade de uma instância com base em testes adicionais fornecidos pelo balanceador de carga. O uso das verificações de integridade do Elastic Load Balancing também ajuda a apoiar a disponibilidade de aplicativos que usam grupos do EC2 Auto Scaling.

Correção

Para adicionar verificações de integridade do Elastic Load Balancing, consulte Adicionar verificações de integridade do Elastic Load Balancing no Guia do usuário do Amazon EC2 Auto Scaling.

[AutoScaling.2] O grupo Amazon EC2 Auto Scaling deve abranger várias zonas de disponibilidade

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra do AWS Config : `autoscaling-multiple-az`

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub	
`minAvailabilityZones`	Número mínimo de zonas de disponibilidade	Enum	`2, 3, 4, 5, 6`	`2`	

Esse controle verifica se um grupo do Amazon EC2 Auto Scaling abrange pelo menos o número especificado de zonas de disponibilidade (AZs). O controle falhará se um grupo do Auto Scaling não abranger pelo menos o número especificado de AZs. A menos que você forneça um valor de parâmetro personalizado para o número mínimo de AZs, o Security Hub usará um valor padrão de duas AZs.

Um grupo do Auto Scaling que não abranja várias AZs não poderá iniciar instâncias em outra AZ para compensar se a única AZ configurada ficar indisponível. Entretanto, um grupo do Auto Scaling com uma única zona de disponibilidade pode ser preferível em alguns casos de uso, como trabalhos em lote ou quando os custos de transferência entre AZs precisam ser reduzidos ao mínimo. Nesses casos, é possível desabilitar esse controle ou suprimir suas descobertas.

Correção

Para adicionar AZs a um grupo do Auto Scaling existente consulte Adicionar e remover zonas de disponibilidade no Guia do usuário do Amazon EC2 Auto Scaling.

[AutoScaling.3] As configurações de lançamento de grupos do Auto Scaling devem configurar as instâncias do EC2 para exigir o Instance Metadata Service Version 2 (IMDSv2)

Requisitos relacionados: NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-11, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-12

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso

Regra do AWS Config : `autoscaling-launchconfig-requires-imdsv2`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o IMDSv2 está habilitado em todas as instâncias iniciadas pelos grupos do Amazon EC2 Auto Scaling. O controle falhará se a versão do serviço de metadados de instância (IMDS) não estiver incluída na configuração de inicialização ou se o IMDSv1 e o IMDSv2 estiverem habilitados.

Os metadados da instância são dados sobre sua instância que é possível usar para configurar ou gerenciar a instância em execução.

A versão 2 do IMDS adiciona novas proteções que não estavam disponíveis no IMDSv1 para proteger ainda mais suas instâncias do EC2.

Correção

Um grupo do Auto Scaling é associado a uma configuração de execução de cada vez. Não é possível modificar uma configuração de execução de uma instância, não é possível modificá-la. Para alterar a configuração de execução para um grupo do Auto Scaling, use uma configuração de execução existente como base para uma nova configuração de execução. Para ter mais informações, consulte Configurar as opções de metadados da instância no Guia do usuário do Amazon EC2 para instâncias Linux.

[AutoScaling.4] A configuração de inicialização do grupo Auto Scaling não deve ter um limite de salto de resposta de metadados maior que 1

> **Important**
>
> O Security Hub retirou esse controle em abril de 2024. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso

Regra do AWS Config : `autoscaling-launch-config-hop-limit`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica o número de saltos de rede que um token de metadados pode percorrer. O controle falhará se o limite de salto de resposta de metadados for maior que 1.

O serviço de metadados de instância (IMDS) fornece informações de metadados sobre uma instância do Amazon EC2 e é útil para configuração de aplicativos. Restringir a resposta HTTP PUT do serviço de metadados somente à instância do EC2 protege o IMDS do uso não autorizado.

O campo Time To Live (TTL) no pacote IP é reduzido em um em cada salto. Essa redução pode ser usada para garantir que o pacote não viaje para fora do EC2. O IMDSv2 protege instâncias do EC2 que podem ter sido configuradas incorretamente como roteadores abertos, firewalls de camada 3, VPNs, túneis ou dispositivos NAT, o que impede que usuários não autorizados recuperem metadados. Com o IMDSv2, a resposta PUT que contém o token secreto não pode sair da instância porque o limite de salto de resposta de metadados padrão está definido como 1. Entretanto, se esse valor for maior que 1, o token poderá sair da instância do EC2.

Correção

Para modificar o limite de salto de resposta de metadados para uma configuração de execução existente, consulte Modificar opções de metadados de instância para instâncias existentes no Guia do usuário do Amazon EC2 para instâncias Linux.

As instâncias do Amazon EC2 lançadas usando as configurações de execução em grupo do Auto Scaling não devem ter endereços IP públicos

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso

Regra do AWS Config : `autoscaling-launch-config-public-ip-disabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se a configuração de inicialização associada a um grupo do Auto Scaling atribui um endereço IP público às instâncias do grupo. O controle falhará se a configuração de inicialização associada atribuir um endereço IP público.

As instâncias do Amazon EC2 em uma configuração de lançamento de grupo do Auto Scaling não devem ter um endereço IP público associado, exceto em casos extremos limitados. As instâncias do Amazon EC2 só devem ser acessíveis por trás de um balanceador de carga, em vez de serem expostas diretamente à internet.

Correção

Um grupo do Auto Scaling é associado a uma configuração de execução de cada vez. Não é possível modificar uma configuração de execução de uma instância, não é possível modificá-la. Para alterar a configuração de execução para um grupo do Auto Scaling, use uma configuração de execução existente como base para uma nova configuração de execução. Em seguida, atualize o grupo do Auto Scaling para usar a nova configuração de execução. Para step-by-step obter instruções, consulte Alterar a configuração de lançamento de um grupo de Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling. Ao criar a nova configuração de execução, em Configuração adicional, para Detalhes avançados, tipo de endereço IP, escolha Não atribuir um endereço IP público a nenhuma instância.

Depois de alterar a configuração de execução, o Ajuste de escala automático inicia novas instâncias com as novas opções de configuração. As instâncias existentes não são afetadas. Para atualizar uma instância existente, recomendamos que você atualize-a ou permita que a escalabilidade automática substitua gradualmente as instâncias mais antigas por instâncias mais novas com base em suas políticas de término. Para obter mais informações sobre a criação de um grupo do Amazon EC2 Auto Scaling, consulte Grupos do Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling.

[AutoScaling.6] Os grupos de Auto Scaling devem usar vários tipos de instância em várias zonas de disponibilidade

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra do AWS Config : `autoscaling-multiple-instance-types`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um grupo do Amazon EC2 Auto Scaling usa vários tipos de instância. O controle falhará se o grupo do Auto Scaling tiver apenas um tipo de instância definido.

É possível aprimorar a disponibilidade ao implantar seu aplicativo em vários tipos de instâncias em execução em várias zonas de disponibilidade. O Security Hub recomenda o uso de vários tipos de instância para que o grupo do Auto Scaling possa executar outro tipo de instância se houver capacidade de instância insuficiente nas zonas de disponibilidade escolhidas.

Correção

Para criar um grupo do Auto Scaling com vários tipos de instância, consulte Grupos do Auto Scaling com vários tipos de instância e opções de compra no Guia do usuário do Amazon EC2 Auto Scaling.

[AutoScaling.9] Os grupos do Amazon EC2 Auto Scaling devem usar os modelos de lançamento do Amazon EC2

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Configuração de recursos

Severidade: média

Tipo de recurso

Regra do AWS Config : `autoscaling-launch-template`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Verifica se um grupo do Amazon EC2 Auto Scaling foi criado de um modelo de inicialização do Amazon EC2. Esse controle falhará se um grupo do Amazon EC2 Auto Scaling não for criado com um modelo de execução ou se um modelo de execução não for especificado em uma política de instâncias mistas.

Ao criar um grupo de Auto Scaling, use um modelo de execução ou uma configuração de execução. Entretanto, usar um modelo de execução para criar um grupo do Auto Scaling garante que você tenha acesso aos recursos e melhorias mais recentes.

Correção

Para criar um grupo do Auto Scaling com um modelo de inicialização do EC2, consulte Criar um grupo do Auto Scaling usando um modelo de execução no Guia do usuário do Amazon EC2 Auto Scaling. Para obter informações sobre como substituir uma configuração de execução por um modelo de execução, consulte Substituir uma configuração de execução por um modelo de execução no Guia do usuário do Amazon EC2 para instâncias do Windows.

[AutoScaling.10] Os grupos do EC2 Auto Scaling devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-autoscaling-autoscalinggroup` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um grupo do Amazon EC2 Auto Scaling tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o grupo Auto Scaling não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro.

`requiredTagKeys` Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o grupo Auto Scaling não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um grupo do Auto Scaling, consulte Grupos e instâncias do Tag Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling.

Amazon EC2 Systems Manager

Esses controles estão relacionados às instâncias do Amazon EC2 que são gerenciadas pelo. AWS Systems Manager

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[SSM.1] As instâncias do Amazon EC2 devem ser gerenciadas por AWS Systems Manager

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Identificar > Inventário

Severidade: média

Recurso avaliado: `AWS::EC2::Instance`

Recursos AWS Config de gravação necessários:`AWS::EC2::Instance`, `AWS::SSM::ManagedInstanceInventory`

Regra do AWS Config : `ec2-instance-managed-by-systems-manager`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se as instâncias do EC2 interrompidas e em execução na sua conta são gerenciadas pelo AWS Systems Manager. O Systems Manager é um AWS service (Serviço da AWS) que você pode usar para visualizar e controlar sua AWS infraestrutura.

Para ajudar você a manter a segurança e a conformidade, o verifica as instâncias gerenciadas. Uma instância gerenciada é uma máquina que foi configurada para uso com o Systems Manager. Em seguida, o Systems Manager relata ou toma medidas corretivas sobre quaisquer violações de políticas detectadas. O Systems Manager também ajuda você a configurar e manter suas instâncias gerenciadas.

Para saber mais, consulte o Manual do usuário do AWS Systems Manager .

Correção

Para gerenciar instâncias do EC2 com o Systems Manager, consulte Gerenciamento de host do Amazon EC2 no Guia do usuário do AWS Systems Manager . Na seção Opções de configuração, é possível manter as opções padrão ou alterá-las conforme necessário para sua configuração preferida.

[PCI.SSM.1] As instâncias do Amazon EC2 gerenciadas pelo devem ter um status de conformidade de patch de COMPLIANT (Em conformidade) após a instalação do patch

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Detectar > Serviços de detecção

Severidade: alta

Tipo de recurso

Regra do AWS Config : `ec2-managedinstance-patch-compliance-status-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o status da conformidade do patch do `COMPLIANT` é ou após a instalação do patch na instância. O controle falhará se o status de conformidade for `NON_COMPLIANT`. Ele verifica somente as instâncias gerenciadas pelo gerenciador de patches do .

Ter as instâncias do EC2 totalmente corrigidas conforme exigido pela organização reduz a superfície de ataque das contas da Contas da AWS.

Correção

O Systems Manager recomenda o uso de políticas de patch para configurar a correção das suas instâncias gerenciadas. Também é possível usar documentos do Systems Manager, conforme descrito no procedimento a seguir, para corrigir uma instância.

Como corrigir patches que não estão em conformidade

1. Abra o AWS Systems Manager console em https://console.aws.amazon.com/systems-manager/.
2. Em Instances & Nodes (Instâncias e nós), escolha Run Command (Executar comando) e Run command (Executar comando).
3. Escolha a opção para AWS- RunPatchBaseline.
4. Altere Operation (Operação) para Install (Instalar).

5. Selecione Choose instances manually (Escolher instâncias manualmente) e selecione as instâncias que não estão em conformidade.
6. Escolha Executar.
7. Após a conclusão do comando, para monitorar o novo status de conformidade das instâncias com patches, no painel de navegação, escolha Compliance (Conformidade).

PCI.SSM.2 As instâncias de Amazon EC2 gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `ec2-managedinstance-association-compliance-status-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o status da conformidade da AWS Systems Manager associação é `COMPLIANT` ou `NON_COMPLIANT` após a execução da associação em uma instância. O controle falhará se o status de conformidade for `NON_COMPLIANT`.

Uma associação do é uma configuração que é atribuída às instâncias gerenciadas. A configuração define o estado que você deseja manter em suas instâncias. Por exemplo, uma associação pode especificar que o software antivírus deve estar instalado e em execução nas instâncias ou que determinadas portas devem ser fechadas.

Depois de criar uma ou mais associações de State Manager, as informações de status de conformidade ficam imediatamente disponíveis para você. Você pode visualizar o status de conformidade no console ou em resposta aos AWS CLI comandos ou às ações correspondentes da API do Systems Manager. Para associações, a Conformidade de configuração mostra o status de conformidade (`Compliant` ou `Non-compliant`). Também mostra o nível de severidade atribuído à associação, como `Critical` ou `Medium`.

Para saber mais sobre a conformidade da associação State Manager, consulte Sobre a conformidade de associações do Gerenciador de Estados no Guia do usuário do AWS Systems Manager .

Correção

Uma associação com falha pode estar relacionada a coisas diferentes, incluindo destinos e nomes de documentos SSM. Para corrigir esse problema, você deve primeiro identificar e investigar a associação visualizando o histórico da associação. Para obter instruções sobre como visualizar o histórico de associações, consulte Visualização de históricos de associações no Guia do usuário do AWS Systems Manager .

Depois de investigar, é possível editar a associação para corrigir o problema identificado. É possível editar uma associação para especificar um novo nome, agendamento, nível de gravidade ou destinos. Depois de editar uma associação, AWS Systems Manager cria uma nova versão. Para obter instruções sobre como editar uma associação, consulte Edita e criar uma nova versão de uma associação no Guia do usuário do AWS Systems Manager .

Os documentos SSM não devem ser públicos

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Configuração de rede segura > Recursos não acessíveis ao público

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `ssm-document-not-public`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se AWS Systems Manager os documentos pertencentes à conta são públicos. Esse controle falhará se os documentos SSM com o proprietário `Self` forem públicos.

Documentos SSM que são públicos podem permitir acesso não intencional aos seus documentos. Um documento SSM público pode expor informações valiosas sobre sua conta, recursos e processos internos.

A menos que seu caso de uso exija compartilhamento público, recomendamos que você bloqueie a configuração de compartilhamento público para documentos do Systems Manager que sejam de propriedade de `Self`.

Correção

Para bloquear o compartilhamento público de documentos SSM, consulte Bloquear compartilhamento público de documentos SSM no Guia do usuário do AWS Systems Manager .

Amazon Elastic File System

Esses controles estão relacionados aos recursos do Amazon EFS resources.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[EFS.1] O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.4.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.R5 SI-7 (6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra do AWS Config : `efs-encrypted-check`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o Amazon Elastic File System está configurado para criptografar os dados do arquivo usando AWS KMS. A verificação falhará nos seguintes casos.

- `Encrypted` está definido como `false` na resposta do `DescribeFileSystems`.
- A chave `KmsKeyId` na resposta do `DescribeFileSystems` não corresponde ao parâmetro `KmsKeyId` para `efs-encrypted-check`.

Observe que esse controle não usa o parâmetro `KmsKeyId` para `efs-encrypted-check`. Ele só verifica o valor de `Encrypted`.

Para obter uma camada de segurança adicional para os dados confidenciais no , crie sistemas de arquivos criptografados. O oferece suporte para sistemas de arquivos em repouso. O Amazon EFS é compatível com sistemas de arquivos criptografados. É possível ativar a criptografia em repouso ao criar um sistema de arquivos do . Para obter mais informações, consulte Criptografia de dados no Amazon EFS no Manual do usuário do Amazon Elastic File System.

Correção

Para obter detalhes sobre como criptografar um novo sistema de arquivos do Amazon EFS , consulte Criptografar dados em repouso no Guia do usuário do Amazon Elastic File System.

[EFS.2] Os volumes do Amazon EFS devem estar em planos de backup

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Recuperação > Resiliência > Backups ativados

Severidade: média

Tipo de recurso

Regra do AWS Config : `efs-in-backup-plan`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se os sistemas de arquivos do Amazon Elastic File System (Amazon EFS) foram adicionados aos planos de backup em AWS Backup. O controle falhará se os sistemas de arquivos do Amazon EFS não estiverem incluídos nos planos de backup.

Incluir sistemas de arquivos EFS nos planos de backup ajuda você a proteger seus dados contra exclusão e perda de dados.

Correção

Para habilitar backups automáticos para um sistema de arquivos Amazon EFS existente, consulte Conceitos básicos 4: Criar backups automáticos do Amazon EFS no Guia do desenvolvedor do AWS Backup .

Os pontos de acesso do EFS devem impor um diretório raiz

Requisitos relacionados: NIST.800-53.r5 CA-7

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `efs-access-point-enforce-root-directory`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os pontos de acesso do Amazon EFS estão configurados para impor um diretório raiz. O controle falhará se o valor de `Path` for definido como `/` (o diretório raiz padrão do sistema de arquivos).

Ao impor um diretório raiz, o cliente NFS usando o ponto de acesso utiliza o diretório raiz configurado no ponto de acesso em vez do diretório raiz do sistema de arquivos. A imposição de um diretório raiz para um ponto de acesso ajuda a restringir o acesso aos dados, garantindo que os usuários do ponto de acesso só possam acessar arquivos do subdiretório especificado.

Correção

Para obter instruções sobre como aplicar um diretório raiz para um ponto de acesso do Amazon EFS, consulte Aplicação de um diretório raiz com um ponto de acesso no Guia do usuário do Amazon Elastic File System.

Os pontos de acesso do EFS devem impor uma identidade de usuário

Requisitos relacionados: NIST.800-53.r5 CA-7

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `efs-access-point-enforce-user-identity`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os pontos de acesso do Amazon EFS estão configurados para impor um diretório raiz. Esse controle falhará se uma identidade de usuário POSIX não for definida durante a criação do ponto de acesso EFS.

Os pontos de acesso do Amazon EFS são pontos de entrada específicos da aplicação para um sistema de arquivos do EFS que facilitam o gerenciamento do acesso de aplicações a conjuntos de dados compartilhados. Os pontos de acesso podem impor uma identidade de usuário, inclusive grupos POSIX do usuário, para todas as solicitações do sistema de arquivamento feitas por meio do ponto de acesso. Os pontos de acesso também podem impor um diretório raiz diferente para o sistema de arquivamento fazendo com que clientes só possam acessar dados no diretório especificado ou em seus subdiretórios.

Correção

Para impor uma identidade de usuário para um ponto de acesso do Amazon EFS, consulte Impor uma identidade de usuário usando um ponto de acesso no Guia do usuário do Amazon Elastic File System.

[EFS.5] Os pontos de acesso do EFS devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config: `tagged-efs-accesspoint` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um ponto de acesso do Amazon EFS tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o ponto de acesso não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o ponto de acesso não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS

Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um ponto de acesso do EFS, consulte Como marcar recursos do Amazon EFS no Guia do usuário do Amazon Elastic File System.

[EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública

Categoria: Proteger > Configuração de rede segura > Recursos não acessíveis ao público

Severidade: média

Tipo de recurso

Regra do AWS Config : `efs-mount-target-public-accessible`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um destino de montagem do Amazon EFS está associado a uma sub-rede privada. O controle falhará se o destino de montagem estiver associado a uma sub-rede pública.

Por padrão, um sistema de arquivos só pode ser acessado a partir da nuvem privada virtual (VPC) na qual você o criou. Recomendamos criar destinos de montagem do EFS em sub-redes privadas que não sejam acessíveis pela Internet. Isso ajuda a garantir que seu sistema de arquivos seja acessível somente a usuários autorizados e não seja vulnerável a acessos ou ataques não autorizados.

Correção

Você não pode alterar a associação entre um destino de montagem do EFS e uma sub-rede depois de criar o destino de montagem. Para associar um destino de montagem existente a uma sub-rede diferente, você deve criar um novo destino de montagem em uma sub-rede privada e, em seguida, remover o destino de montagem antigo. Para obter informações sobre o gerenciamento de alvos de montagem, consulte Criação e gerenciamento de alvos de montagem e grupos de segurança no Guia do usuário do Amazon Elastic File System.

Amazon Elastic Kubernetes Service

Esses controles estão relacionados aos recursos da Amazon EKS.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

Os endpoints do cluster EKS não devem ser acessíveis ao público

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Gerenciamento de acesso seguro > Recursos não acessíveis ao público

Severidade: alta

Tipo de recurso

Regra do AWS Config : `eks-endpoint-no-public-access`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um endpoint de cluster Amazon EKS está acessível publicamente. O controle falhará se um cluster EKS tiver um endpoint acessível ao público.

Quando você cria um cluster, o Amazon EKS cria um endpoint para o servidor gerenciado de API do Kubernetes usado para se comunicar com o cluster (usando as ferramentas de gerenciamento do Kubernetes, como). Por padrão, esse endpoint do servidor de API está disponível publicamente na internet. O acesso ao servidor da API é protegido usando uma combinação do AWS Identity and Access Management (IAM) e do Kubernetes Role Based Access Control (RBAC) nativo. Ao remover o acesso público ao endpoint, é possível evitar a exposição e o acesso não intencionais ao seu cluster.

Correção

Para modificar o acesso ao endpoint para um cluster EKS existente, consulte Modificar o acesso ao endpoint do cluster no Guia do usuário do Amazon EKS. É possível configurar o acesso ao endpoint

para um novo cluster EKS ao criá-lo. Para obter instruções sobre como criar um novo cluster do Amazon EKS, consulte Criar um cluster do Amazon EKS no Guia do usuário do Amazon EKS.

Os clusters EKS devem ser executados em uma versão compatível do Kubernetes

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Detectar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: alta

Tipo de recurso

Regra do AWS Config : `eks-cluster-supported-version`

Tipo de programação: acionado por alterações

Parâmetros:

- `oldestVersionSupported`: `1.26` (não personalizável)

Esse controle verifica se um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) está sendo executado em uma versão do Kubernetes com suporte. O controle falhará se o cluster EKS estiver sendo executado em uma versão não compatível.

Se a sua aplicação não exigir uma versão específica do , recomendamos que você use a versão do mais recente disponível compatível com o Amazon EKS para seus clusters. Para obter mais informações, consulte o calendário de lançamento do Amazon EKS Kubernetes e o Suporte à versão do Amazon EKS e perguntas frequentes no Guia do usuário do Amazon EKS.

Correção

Para atualizar um cluster EKS, Atualizar uma versão Kubernetes de um cluster do Amazon EKS no Guia do usuário do Amazon EKS.

[EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes

Requisitos relacionados: NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-13, Nist.800-53.r5 SI-28

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra do AWS Config : `eks-secrets-encrypted`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um cluster Amazon EKS usa segredos criptografados do Kubernetes. O controle falhará se os segredos do Kubernetes do cluster não estiverem criptografados.

Ao criptografar segredos, você pode usar as chaves AWS Key Management Service (AWS KMS) para fornecer criptografia de envelope dos segredos do Kubernetes armazenados no etcd para seu cluster. Essa criptografia é adicional à criptografia de volume do EBS que é ativada por padrão para todos os dados (incluindo segredos) armazenados no etcd como parte de um cluster EKS. O uso da criptografia de segredos para seu cluster EKS permite implantar uma estratégia de defesa aprofundada para aplicativos Kubernetes, criptografando segredos do Kubernetes com uma chave KMS que você define e gerencia.

Correção

Para habilitar a criptografia secreta em um cluster EKS, consulte Como ativar a criptografia secreta em um cluster existente no Guia do usuário do Amazon EKS.

[EKS.6] Os clusters EKS devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config: `tagged-eks-cluster` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um cluster do Amazon EKS tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o cluster não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o cluster não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS

Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um cluster do EKS, consulte Como marcar seus recursos do Amazon EKS no Guia do usuário do Amazon EKS.

[EKS.7] As configurações do provedor de identidade EKS devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config: `tagged-eks-identityproviderconfig` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se a configuração de um provedor de identidade do Amazon EKS tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a configuração não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só

verificará a existência de uma chave de tag e falhará se a configuração não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags às configurações de um provedor de identidade EKS, consulte Como marcar seus recursos do Amazon EKS no Guia do usuário do Amazon EKS.

[EKS.8] Os clusters do EKS devem ter o registro em log de auditoria habilitado

Requisitos relacionados: CIS Foundations Benchmark v1.2.0/2.1, CIS Foundations Benchmark v1.4.0/3.1, NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-14(1), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8), NIST.800-53.r5 SA-8(22)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `eks-cluster-logging-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um cluster do Amazon EKS tem o registro em log de auditoria habilitado. O controle falhará se o registro em log de auditoria não estiver habilitado para o cluster.

O registro do plano de controle do EKS fornece registros de auditoria e diagnóstico diretamente do plano de controle do EKS para o Amazon CloudWatch Logs em sua conta. Você pode selecionar os tipos de registro necessários e os registros são enviados como fluxos de log para um grupo para cada cluster EKS em CloudWatch. O registro em log fornece visibilidade sobre o acesso e a performance dos clusters EKS. Ao enviar registros do plano de controle EKS para seus clusters EKS para o CloudWatch Logs, você pode registrar operações para fins de auditoria e diagnóstico em um local central.

Correção

Para habilitar registros em log de auditoria para seu cluster do EKS, consulte Habilitação e desabilitação de logs do ambiente de gerenciamento no Guia do usuário do Amazon EKS.

ElastiCache Controles da Amazon

Esses controles estão relacionados aos ElastiCache recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[ElastiCache.1] Os clusters ElastiCache Redis devem ter o backup automático ativado

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Recuperação > Resiliência > Backups ativados

Severidade: alta

Tipo de recurso

AWS Config regra: **elasticache-redis-cluster-automatic-backup-check**

Tipo de programação: Periódico

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`snapshotRetentionPeriod`	Período mínimo de retenção de snapshot em dias	Inteiro	1 para 35	1

Esse controle avalia se um cluster Amazon ElastiCache for Redis tem backups automáticos programados. O controle falhará se o `SnapshotRetentionLimit` para o cluster do Redis menor que o período de tempo especificado. A menos que você forneça um valor de parâmetro personalizado para o período de retenção do snapshot, o Security Hub usará um valor padrão de 1 dia.

Os clusters Amazon ElastiCache for Redis podem fazer backup de seus dados. O backup pode ser usado para restaurar um cluster ou propagar um novo cluster. O backup consiste nos metadados do cluster, juntamente com todos os dados do cluster. Todos os backups são gravados no Amazon Simple Storage Service (Amazon S3), que fornece armazenamento durável. A qualquer momento, é possível restaurar seus dados criando um novo cluster Redis e preenchendo-o com dados de um backup. Você pode gerenciar backups usando o AWS Management Console, o AWS Command Line Interface (AWS CLI) e a ElastiCache API.

Correção

Para programar backups automáticos em um cluster ElastiCache para Redis, consulte Programação de backups automáticos no Guia ElastiCache do usuário da Amazon.

[ElastiCache.2] ElastiCache para clusters de cache Redis deve ter a atualização automática de versão secundária habilitada

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Detectar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: alta

Tipo de recurso

Regra do AWS Config : `elasticache-auto-minor-version-upgrade-check`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle avalia se ElastiCache o Redis aplica automaticamente atualizações de versões secundárias aos clusters de cache. Esse controle falhará se ElastiCache os clusters de cache do Redis não tiverem atualizações de versão menores aplicadas automaticamente.

`AutoMinorVersionUpgrade`é um recurso que você pode ativar no Redis ElastiCache para que seus clusters de cache sejam atualizados automaticamente quando uma nova versão secundária do mecanismo de cache estiver disponível. incluem os patches de segurança e as correções de erros mais recentes. Continuar up-to-date com a instalação do patch é uma etapa importante para proteger os sistemas.

Correção

Para aplicar atualizações automáticas de versões secundárias a um cluster de cache existente ElastiCache para Redis, consulte Atualização de versões do mecanismo no Guia do usuário da Amazon ElastiCache .

[ElastiCache.3] ElastiCache para grupos de replicação do Redis, o failover automático deve estar ativado

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra do AWS Config : `elasticache-repl-grp-auto-failover-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se os grupos ElastiCache de replicação do Redis têm o failover automático ativado. Esse controle falhará se o failover automático não estiver habilitado para um grupo de replicação do Redis.

Quando o failover automático é habilitado para um grupo de replicação, a função do nó primário fará failover automaticamente para uma das réplicas de leitura. O failover e a promoção de réplica garantem que você possa continuar a gravar no novo primário assim que a promoção estiver concluída.

Correção

Para habilitar o failover automático para um grupo de replicação existente ElastiCache para Redis, consulte Modificação de um cluster ElastiCache no Guia do usuário da Amazon. ElastiCache Se você usa o ElastiCache console, defina o failover automático como ativado.

[ElastiCache.4] ElastiCache para Redis, os grupos de replicação devem ser criptografados em repouso

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso

Regra do AWS Config : `elasticache-repl-grp-encrypted-at-rest`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se os grupos ElastiCache de replicação do Redis estão criptografados em repouso. Esse controle falhará se um grupo de replicação ElastiCache for Redis não estiver criptografado em repouso.

Criptografar dados em repouso reduz o risco de um usuário não autenticado ter acesso aos dados armazenados em disco. ElastiCache para Redis, os grupos de replicação devem ser criptografados em repouso para uma camada adicional de segurança.

Correção

Para configurar a criptografia em repouso em um grupo de replicação ElastiCache para Redis, consulte Habilitar a criptografia em repouso no Guia do usuário da Amazon. ElastiCache

[ElastiCache.5] ElastiCache para Redis, os grupos de replicação devem ser criptografados em trânsito

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso

Regra do AWS Config : `elasticache-repl-grp-encrypted-in-transit`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se ElastiCache os grupos de replicação do Redis estão criptografados em trânsito. Esse controle falhará se um grupo de replicação ElastiCache for Redis não estiver criptografado em trânsito.

Criptografar dados em trânsito reduz o risco de um usuário não autorizado espionar o tráfego da rede. Habilitar a criptografia em trânsito em um ElastiCache grupo de replicação do Redis criptografa seus dados sempre que eles são movidos de um lugar para outro, como entre os nós do cluster ou entre o cluster e o aplicativo.

Correção

Para configurar a criptografia em trânsito em um grupo de replicação ElastiCache para Redis, consulte Habilitar a criptografia em trânsito no Guia do usuário da Amazon. ElastiCache

[ElastiCache.6] ElastiCache para grupos de replicação do Redis antes da versão 6.0 deve usar o Redis AUTH

Requisitos relacionados: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `elasticache-repl-grp-redis-auth-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se os grupos ElastiCache de replicação do Redis têm o Redis AUTH ativado. O controle falhará em um grupo de replicação ElastiCache for Redis se a versão Redis de seus nós estiver abaixo de 6.0 e `AuthToken` não estiver em uso.

Os tokens de autenticação do Redis, ou senhas, habilitam o Redis a exigir uma senha antes de permitir que os clientes executem comandos, melhorando assim a segurança dos dados. Para o Redis 6.0 e versões posteriores, recomendamos o uso do Role-Based Access Control (RBAC — Controle de acesso baseado em perfil). Como o RBAC não é compatível com versões do Redis anteriores à 6.0, esse controle avalia apenas as versões que não podem usar o atributo RBAC.

Correção

Para usar o Redis AUTH em um ElastiCache grupo de replicação do Redis, consulte Modificação do token AUTH em um cluster existente do ElastiCache Redis no Guia do usuário da Amazon. ElastiCache

[ElastiCache.7] os ElastiCache clusters não devem usar o grupo de sub-rede padrão

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso

Regra do AWS Config : `elasticache-subnet-group-check`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se os ElastiCache clusters estão configurados com um grupo de sub-rede personalizado. O controle falhará para um ElastiCache cluster se `CacheSubnetGroupName` tiver o valor`default`.

Ao iniciar um ElastiCache cluster, um grupo de sub-rede padrão é criado, caso ainda não exista um. O grupo padrão usa sub-redes da Nuvem privada virtual (VPC) padrão. Recomendamos usar grupos de sub-redes personalizados que sejam mais restritivos em relação às sub-redes em que o cluster reside e à rede que o cluster herda das sub-redes.

Correção

Para criar um novo grupo de sub-redes para um ElastiCache cluster, consulte Criação de um grupo de sub-redes no Guia ElastiCache do usuário da Amazon.

AWS Elastic Beanstalk controles

Esses controles estão relacionados aos recursos do Elastic Beanstalk.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de integridade aprimorados habilitados

Requisitos relacionados: NIST.800-53.r5 SI-4 (12), NIST.800-53.r5 SI-4 (5)

Categoria: Detectar > Serviços de detecção > Monitoramento de aplicativos

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `beanstalk-enhanced-health-reporting-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os relatórios de integridade aprimorados estão habilitados para seus ambientes AWS Elastic Beanstalk .

Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às alterações na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo.

Os relatórios de saúde aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a severidade dos problemas identificados e identificar possíveis causas a serem investigadas. O agente de integridade do Elastic Beanstalk, incluído nas imagens de máquina da Amazon (AMIs) suportadas, avalia logs e métricas das instâncias EC2 do ambiente.

Para obter informações adicionais, consulte Monitoramento e relatório de integridade aprimorada no Guia do desenvolvedor do AWS Elastic Beanstalk .

Correção

Para obter instruções sobre como habilitar relatórios de saúde aprimorados, consulte Habilitar relatórios de integridade aprimorada usando o console do Elastic Beanstalk no Guia do desenvolvedor do AWS Elastic Beanstalk .

[ElasticBeanstalk.2] As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Detectar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: alta

Tipo de recurso

Regra do AWS Config : `elastic-beanstalk-managed-updates-enabled`

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`UpdateLevel`	Nível de atualização da versão	Enum	`minor`, `patch`	Nenhum valor padrão

Esse controle verifica se as atualizações da plataforma gerenciadas estão habilitadas para o ambiente do Elastic Beanstalk. O controle falhará se nenhuma atualização da plataforma gerenciada estiver habilitada. Por padrão, o controle passará se algum tipo de atualização da plataforma estiver habilitado. Opcionalmente, é possível fornecer um valor de parâmetro personalizado para exigir um nível de atualização específico.

A ativação das atualizações gerenciadas da plataforma garante que as correções, atualizações e recursos mais recentes da plataforma disponíveis para o ambiente sejam instalados. Manter-se atualizado com a instalação do patch é uma etapa importante para proteger os sistemas.

Correção

Para permitir atualizações da plataforma gerenciadas, consulte Para configurar atualizações da plataforma gerenciadas em Atualizações da plataforma gerenciadas no Guia do desenvolvedor do AWS Elastic Beanstalk .

[ElasticBeanstalk.3] O Elastic Beanstalk deve transmitir registros para CloudWatch

Categoria: Identificar > Registro em log

Severidade: alta

Tipo de recurso

Regra do AWS Config : `elastic-beanstalk-logs-to-cloudwatch`

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`RetentionInDays`	Número de dias para manter eventos de log antes que expirem	Enum	`1`, `3`, `5`, `7`, `14`, `30`, `60`, `90`, `120`, `150`, `180`, `365` , `400`, `545`, `731`, `1827`, `3653`	Nenhum valor padrão

Esse controle verifica se um ambiente do Elastic Beanstalk está configurado para enviar registros para o Logs. CloudWatch O controle falhará se um ambiente do Elastic Beanstalk não estiver configurado para enviar registros para o Logs. CloudWatch Opcionalmente, é possível fornecer um valor personalizado para o parâmetro `RetentionInDays` se quiser que o controle passe somente se os logs forem retidos pelo número especificado de dias antes da expiração.

CloudWatch ajuda você a coletar e monitorar várias métricas para seus aplicativos e recursos de infraestrutura. Você também pode usar CloudWatch para configurar ações de alarme com base em métricas específicas. Recomendamos integrar o Elastic CloudWatch Beanstalk para obter maior visibilidade do seu ambiente do Elastic Beanstalk. Os logs do Elastic Beanstalk incluem o eb-activity.log, logs de acesso do ambiente nginx ou do servidor proxy Apache e logs específicos de um ambiente.

Correção

Para integrar o Elastic CloudWatch Beanstalk com o Logs, consulte Streaming de registros de instâncias para CloudWatch registros no Guia do desenvolvedor.AWS Elastic Beanstalk

Elastic Load Balancing Concepts (Conceitos do Elastic Load Balancing)

Esses controles estão relacionados aos recursos do Elastic Beanstalk.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[ELBv2.1] O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Detectar > Serviços de detecção

Severidade: média

Tipo de recurso

Regra do AWS Config : `alb-http-to-https-redirection-check`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o redirecionamento HTTP para HTTPS está configurado em todos os listeners HTTP de . O controle falhará se algum dos receptores HTTP dos Application Load Balancers não tiver o redirecionamento de HTTP para HTTPS configurado.

Antes de começar a usar seu Application Load Balancer, você deve adicionar ao menos um receptor. Um listener é um processo que usa o protocolo e a porta configurados para verificar solicitações de conexão. Os listeners oferecem suporte para os protocolos HTTP e HTTPS. É possível usar um listener HTTPS para descarregar o trabalho de criptografia e descriptografia para o . Use as ações de redirecionamento com o para redirecionar uma solicitação HTTP do cliente para uma solicitação do HTTPS na porta 443 para aplicar a criptografia em trânsito.

Para obter mais informações, consulte Criar um listener no Application Load Balancer no Guia do usuário dos Application Load Balancers.

Correção

Para redirecionar solicitações HTTP para HTTPS, você deve adicionar uma regra de receptor do Application Load Balancer ou editar uma regra existente.

Para obter instruções sobre como adicionar uma nova regra, consulte Adicionar uma regra no Guia do usuário dos Application Load Balancers. Insira para Port (Porta), escolha para Protocol

(Protocolo) e depois escolha . Em Adicionar ação, Redirecionar para, escolha HTTPS e, em seguida, insira **443**.

Para obter instruções sobre como adicionar uma nova regra, consulte Adicionar uma regra no Guia do usuário dos Application Load Balancers. Insira para Port (Porta), escolha para Protocol (Protocolo) e depois escolha . Em Adicionar ação, Redirecionar para, escolha HTTPS e, em seguida, insira **443**.

[ELB.2] Os balanceadores de carga clássicos com ouvintes SSL/HTTPS devem usar um certificado fornecido pelo AWS Certificate Manager

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em trânsito

Severidade: média

Tipo de recurso

Regra do AWS Config : `elb-acm-certificate-required`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Verifica se os Classic Load Balancers usam certificados SSL fornecidos pelo AWS Certificate Manager . O controle falhará se o Classic Load Balancer configurado com o receptor de HTTPS/SSL não usar um certificado fornecido pelo ACM.

É possível criar um certificado usando o ACM ou uma ferramenta que ofereça suporte aos protocolos SSL e TLS, como OpenSSL. Recomendamos que você use o (ACM) para criar ou importar certificados para o balanceador de carga.

O ACM se integra ao Elastic Load Balancing para que você possa implantar o certificado em seu balanceador de carga. Você também deve renovar automaticamente esses certificados.

Correção

Para obter informações sobre como associar um certificado SSL/TLS do ACM a um Classic Load Balancer, consulte o artigo do AWS Knowledge Center How can I associate an ACM SSL/TLS certificate with a Classic, Application, or Network Load Balancer?

Os receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em trânsito

Severidade: média

Tipo de recurso

Regra do AWS Config : `elb-tls-https-listeners-only`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se seus receptores do Classic Load Balancer estão configurados com o protocolo HTTPS ou TLS para conexões front-end (cliente para balanceador de carga). O controle é aplicável se um Classic Load Balancer tiver receptores. Se o Classic Load Balancer não tiver um receptor configurado, o controle não relatará nenhuma descoberta.

O controle passa se os receptores do Classic Load Balancer estiverem configurados com TLS ou HTTPS para conexões front-end.

O controle passa se os receptores do Classic Load Balancer estiverem configurados com TLS ou HTTPS para conexões front-end.

Antes de começar a usar o , você deve adicionar um ou mais listeners. Um listener é um processo que usa o protocolo e a porta configurados para verificar solicitações de conexão. Os listeners são compatíveis com os protocolos HTTP e HTTPS. Você deve sempre usar um receptor HTTPS ou TLS, para que o balanceador de carga faça o trabalho de criptografia e descriptografia em trânsito.

Correção

Para corrigir esse problema, atualize seus receptores para usar o protocolo TLS ou HTTPS.

Para alterar todos os receptores não compatíveis para receptores TLS/HTTPS

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Load Balancing, selecione Load Balancers.
3. Selecione seu Classic Load Balancer.
4. Na guia Listeners, selecione Editar.
5. Para todos os receptores em que o Protocolo balanceador de carga não está definido como HTTPS ou SSL, altere a configuração para HTTPS ou SSL.
6. Para todos os receptores modificados, na guia Certificados, escolha Alterar padrão.
7. Em Certificados do ACM e do IAM, selecione um certificado.
8. Escolha Salvar como padrão.
9. Depois de atualizar todos os receptores, escolha Salvar.

O Application Load Balancer deve ser configurado para eliminar cabeçalhos http

Requisitos relacionados: NIST.800-53.r5 SC-28 (3), NIST.800-53.r5 SC-7 (16)

Categoria: Proteger > Segurança de rede

Severidade: média

Tipo de recurso

Regra do AWS Config : `alb-http-drop-invalid-header-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle avalia os AWS Application Load Balancers para garantir que eles estejam configurados para eliminar cabeçalhos HTTP inválidos. O controle falha se `routing.http.drop_invalid_header_fields.enabled` estiver definido como `false`.

Por padrão, os Application Load Balancers não estão configurados para eliminar valores de cabeçalho HTTP inválidos. A remoção desses valores de cabeçalho evita ataques de dessincronização de HTTP.

Observe que é possível desativar esse controle se o ELB.12 estiver ativado.

Correção

Para corrigir esse problema, configure seu balanceador de carga para eliminar campos de cabeçalho inválidos.

Para corrigir esse problema, configure seu balanceador de carga para eliminar campos de cabeçalho inválidos.

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, escolha Load balancers.
3. Excluir um Application Load Balancer
4. Em Ações, escolha Editar atributos.
5. Em Eliminar campos de cabeçalho inválidos, escolha Habilitar.
6. Escolha Salvar.

O registro em log do Classic Load Balancer e Application Load Balancer deve estar ativado

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `elb-logging-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o Application Load Balancer e o Classic Load Balancer têm o registro em log ativado. O controle falha se `access_logs.s3.enabled` estiver definido como `false`.

O Elastic Load Balancing fornece logs de acesso que capturam informações detalhadas sobre as solicitações enviadas ao seu balanceador de carga. Cada log contém informações como a hora

em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor. É possível usar esses logs de acesso para analisar padrões de tráfego e solucionar problemas.

Para obter mais informações, consulte Marcar o Classic Load Balancer no Guia do usuário dos Classic Load Balancers.

Correção

Para ativar os registros de acesso, consulte Etapa 3: Configurar logs de acesso no Guia do usuário dos Application Load Balancers.

[ELB.6] Os balanceadores de carga de aplicativos, gateways e redes devem ter a proteção contra exclusão ativada

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra do AWS Config : `elb-deletion-protection-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um Application, Gateway ou Network Load Balancer tem a proteção contra exclusão ativada. O controle falhará se a proteção contra exclusão estiver desativada.

Ative a proteção contra exclusão para proteger seu aplicativo, gateway ou Network Load Balancer da exclusão.

Correção

Para evitar que seu load balancer seja excluído acidentalmente, é possível ativar a proteção contra exclusão. Por padrão, a proteção contra exclusão está desativada para seu load balancer.

Se você ativar a proteção contra exclusão para o load balancer, deverá desativá-la antes de excluir o load balancer.

Para ativar a proteção contra exclusão em um Application Load Balancer, consulte Proteção contra exclusão no Guia do usuário de Application Load Balancers. Para ativar a proteção contra exclusão para um Gateway Load Balancer, consulte Proteção contra exclusão no Guia do usuário para Gateway Load Balancers. Para ativar a proteção contra exclusão em um Network Load Balancer, consulte Proteção contra exclusão no Guia do usuário para Network Load Balancers.

Os Classic Load Balancers devem ter a drenagem da conexão ativada

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Recuperação > Resiliência

Severidade: média

Tipo de recurso

Regra AWS Config: `elb-connection-draining-enabled` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os Classic Load Balancers têm drenagem da conexão habilitada.

Habilitar a drenagem da conexão em Classic Load Balancers garante que o balanceador de carga interromperá o envio de solicitações para instâncias cujo registro está sendo cancelado ou que não sejam íntegras. Ele mantém as conexões existentes abertas. Isso é particularmente útil para instâncias em grupos do Auto Scaling, para garantir que as conexões não sejam interrompidas abruptamente.

Correção

Para habilitar a drenagem da conexão em Classic Load Balancers, consulte Configurar a drenagem da conexão para o Classic Load Balancer no Guia do usuário dos Classic Load Balancers.

[ELB.8] Os balanceadores de carga clássicos com ouvintes SSL devem usar uma política de segurança predefinida que tenha uma duração forte AWS Config

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em trânsito

Severidade: média

Tipo de recurso

Regra do AWS Config : `elb-predefined-security-policy-ssl-check`

Tipo de programação: acionado por alterações

Parâmetros:

- `predefinedPolicyName`: `ELBSecurityPolicy-TLS-1-2-2017-01` (não personalizável)

Esse controle verifica se os receptores HTTPS/SSL do Classic Load Balancer usam a política predefinida `ELBSecurityPolicy-TLS-1-2-2017-01`. O controle falhará se os receptores HTTPS/SSL do Classic Load Balancer não usarem `ELBSecurityPolicy-TLS-1-2-2017-01`.

A política de segurança é uma combinação de protocolos SSL, cifras SSL e a opção Preferência ditada pelo servidor. Políticas predefinidas controlam as cifras, os protocolos e as ordens de preferência a serem suportadas durante as negociações de SSL entre um cliente e um balanceador de carga.

O uso de `ELBSecurityPolicy-TLS-1-2-2017-01` pode ajudá-lo a atender aos padrões de conformidade e segurança que exigem a desativação de versões específicas de SSL e TLS. Para obter mais informações, consulte Listeners para o Classic Load Balancer no Guia do usuário dos Classic Load Balancers.

Correção

Para obter informações sobre como usar a política de segurança predefinida `ELBSecurityPolicy-TLS-1-2-2017-01` com um Classic Load Balancer, consulte Definir configurações de segurança no Guia do usuário dos Classic Load Balancers.

Os Classic Load Balancers devem ter o balanceador de carga entre zonas habilitado

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra do AWS Config : `elb-cross-zone-load-balancing-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o balanceamento de carga entre zonas está habilitado para os Classic Load Balancers (CLBs). O controle falhará se o balanceamento de carga entre zonas não estiver habilitado para um CLB.

Cada nó de load balancer distribui tráfego para destinos registrados somente na sua Zona de disponibilidade. Quando o balanceamento de carga entre zonas estiver desabilitado, cada nó do load balancer distribuirá o tráfego somente para os destinos registrados na respectiva zona de disponibilidade. Se o número de destinos registrados não for o mesmo nas zonas de disponibilidade, o tráfego não será distribuído uniformemente e as instâncias em uma zona poderão acabar sendo superutilizadas em comparação com as instâncias em outra zona. Com o balanceamento de carga entre zonas, cada nó do balanceador de carga do seu Classic Load Balancer distribui solicitações uniformemente a todas as instâncias registradas em todas as zonas de disponibilidade habilitadas. Para mais informações, consulte Balanceamento de carga entre zonas no Manual do usuário do Elastic Load Balancing.

Correção

Para habilitar o balanceamento de carga entre zonas em um Classic Load Balancer, consulte Habilitar balanceamento de carga entre zonas no Guia do usuário dos Classic Load Balancers.

Verifica se o Classic Load Balancer abrange várias zonas de disponibilidade (AZs).

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra do AWS Config : `clb-multiple-az`

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`minAvailabilityZones`	Número mínimo de zonas de disponibilidade	Enum	`2, 3, 4, 5, 6`	`2`

Esse controle verifica se um Classic Load Balancer foi configurado para abranger ao menos o número especificado de zonas de disponibilidade (AZs). O controle falhará se o Classic Load Balancer não abranger pelo menos o número especificado de AZs. A menos que você forneça um valor de parâmetro personalizado para o número mínimo de AZs, o Security Hub usará um valor padrão de duas AZs.

É possível configurar o Classic Load Balancer no Amazon EC2-Classic para distribuir as solicitações de entrada em instâncias EC2 em uma única Zona de disponibilidade ou em várias Zonas de disponibilidade. Um Classic Load Balancer que não abrange várias zonas de disponibilidade não consegue redirecionar o tráfego para destinos em outra zona de disponibilidade se a única zona de disponibilidade configurada ficar indisponível.

Correção

Para adicionar zonas de disponibilidade a um Classic Load Balancer, consulte Adicionar ou remover sub-redes para seu Classic Load Balancer no Guia do usuário de Classic Load Balancers.

O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso

Requisitos relacionados: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6

Categoria: Proteção de dados > Integridade dos dados

Severidade: média

Tipo de recurso

Regra do AWS Config : `alb-desync-mode-check`

Tipo de programação: acionado por alterações

Parâmetros:

- `desyncMode`: `defensive, strictest` (não personalizável)

O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso O controle falhará se um Application Load Balancer não estiver configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso.

Problemas de dessincronização de HTTP podem levar ao contrabando de solicitações e tornar os aplicativos vulneráveis ao envenenamento da fila de solicitações ou do cache. Por sua vez, essas vulnerabilidades podem levar ao preenchimento de credenciais ou à execução de comandos não autorizados. Os Application Load Balancers configurados com o modo defensivo ou de mitigação de dessincronização mais rigorosa protegem seu aplicativo contra problemas de segurança que podem ser causados pela dessincronização HTTP.

Correção

Para atualizar o modo de mitigação de dessincronização de um Application Load Balancer, consulte Modo de mitigação de dessincronização no Guia do usuário dos Application Load Balancers.

Balanceadores de carga de aplicações, redes e gateways não abrangem várias zonas de disponibilidade

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra do AWS Config : `elbv2-multiple-az`

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`minAvailabilityZones`	Número mínimo de zonas de disponibilidade	Enum	`2, 3, 4, 5, 6`	2

Esse controle verifica se um Elastic Load Balancer V2 (balanceador de carga de aplicação, rede ou gateway) registrou instâncias de ao menos o número especificado de zonas de disponibilidade (AZs). O controle falhará se um Elastic Load Balancer V2 não tiver instâncias registradas em pelo menos o número especificado de AZs. A menos que você forneça um valor de parâmetro personalizado para o número mínimo de AZs, o Security Hub usará um valor padrão de duas AZs.

O Elastic Load Balancing distribui automaticamente seu tráfego de entrada entre vários destinos, como instâncias do EC2, contêineres e endereços IP, em uma ou mais zonas de disponibilidade. O Elastic Load Balancing escala seu balanceador de carga conforme seu tráfego de entrada muda com o tempo. É recomendável configurar pelo menos duas zonas de disponibilidade para garantir a disponibilidade dos serviços, pois o Elastic Load Balancer poderá direcionar o tráfego para outra zona de disponibilidade se uma ficar indisponível. Ter várias zonas de disponibilidade configuradas ajudará a eliminar um único ponto de falha para o aplicativo.

Correção

Para adicionar uma zona de disponibilidade a um Application Load Balancer, consulte Zonas de disponibilidade para Application Load Balancer no Guia do usuário dos Application Load Balancers. Para criar uma Zona de disponibilidade em um Network Load Balancer load balancer de rede, consulte Conceitos básicos sobre load balancers de rede no Guia do usuário do load balancer de rede. Para adicionar uma zona de disponibilidade a um Gateway Load Balancer, consulte Criar um Gateway Load Balancer no Guia do usuário dos Gateway Load Balancers.

O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso

Requisitos relacionados: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6

Categoria: Proteção de dados > Integridade dos dados

Severidade: média

Tipo de recurso

Regra do AWS Config : `clb-desync-mode-check`

Tipo de programação: acionado por alterações

Parâmetros:

- `desyncMode`: `defensive, strictest` (não personalizável)

O controle falhará se um Application Load Balancer não estiver configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso. O controle falhará se um Classic Load Balancer não estiver configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso.

Problemas de dessincronização de HTTP podem levar ao contrabando de solicitações e tornar os aplicativos vulneráveis ao envenenamento da fila de solicitações ou do cache. Por sua vez, essas vulnerabilidades podem levar ao preenchimento de credenciais ou à execução de comandos não autorizados. Os Application Load Balancers configurados com o modo defensivo ou de mitigação de dessincronização mais rigorosa protegem seu aplicativo contra problemas de segurança que podem ser causados pela dessincronização HTTP.

Correção

Para atualizar o modo de mitigação de dessincronização de um Classic Load Balancer, consulte Modo de mitigação de dessincronização no Guia do usuário dos Classic Load Balancers.

[ELB.16] Os balanceadores de carga de aplicativos devem ser associados a uma ACL da web AWS WAF

Requisitos relacionados: NIST.800-53.r5 CA-7

Categoria: Proteger > Serviços de proteção

Severidade: média

Tipo de recurso

Regra do AWS Config : `alb-waf-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um Application Load Balancer está associado a uma lista de controle de acesso AWS WAF clássica ou à AWS WAF web (web ACL). O controle falhará se o campo `Enabled` da configuração AWS WAF estiver definido como `false`.

AWS WAF é um firewall de aplicativos da web que ajuda a proteger aplicativos e APIs da web contra ataques. Com AWS WAF, você pode configurar uma ACL da web, que é um conjunto de regras que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Recomendamos associar seu Application Load Balancer a uma ACL da web do AWS WAF para ajudar a protegê-lo contra ataques maliciosos.

Correção

Para associar um Application Load Balancer a uma ACL da web, consulte Como associar ou desassociar uma ACL da web a um recurso no Guia do desenvolvedor. AWS AWS WAF

Controles do Amazon EMR

Esses controles estão relacionados aos recursos do Amazon EMR.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[EMR.1] Os nós primários do cluster do Amazon EMR não devem ter endereços IP públicos

Requisitos relacionados: PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/1.3.2,PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso

Regra do AWS Config : `emr-master-no-public-ip`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se os nós principais nos clusters do Amazon EMR têm endereços IP públicos. O controle falhará se os endereços IP públicos estiverem associados a qualquer uma das instâncias do nó principal.

Os endereços IP públicos são designados no campo `PublicIp` da configuração `NetworkInterfaces` da instância. Esse controle verifica somente os clusters do Amazon EMR que estão em um estado `RUNNING` ou `WAITING`.

Correção

É possível controlar se sua instância em uma sub-rede padrão ou não padrão é atribuída a um endereço IPv4 público durante a inicialização. Por padrão, as sub-redes padrão têm esse atributo definido como `true`. As sub-redes não padrão têm o atributo de endereçamento público IPv4 configurado como `false`, a menos que ele tenha sido criado pelo assistente de inicialização de instâncias do Amazon EC2. Nesse caso, o atributo é definido como `true`.

Você não pode desassociar manualmente o endereço público IPv4 da sua instância após a inicialização.

Para corrigir uma falha na descoberta, você deve iniciar um novo cluster em uma VPC com uma sub-rede privada que tenha o atributo de endereçamento público IPv4 definido como `false`. Para obter mais informações, consulte Executar clusters do Amazon EMR em uma VPC no Guia de gerenciamento do Amazon EMR.

[EMR.2] A configuração de bloqueio de acesso público do Amazon EMR deve estar habilitada

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Gerenciamento de acesso seguro > Recursos não acessíveis ao público

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `emr-block-public-access`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se sua conta está configurada com o bloqueio de acesso público do Amazon EMR. O controle falhará se a configuração de bloqueio de acesso público não estiver habilitada ou se qualquer porta diferente da porta 22 for permitida.

O bloqueio de acesso público do Amazon EMR impede que você inicie um cluster em uma sub-rede pública se o cluster tiver uma configuração de segurança que permita tráfego de entrada de endereços IP públicos em uma porta. Quando um usuário de sua Conta da AWS inicia um cluster, o Amazon EMR verifica as regras de porta no grupo de segurança do cluster e as compara com as regras de tráfego de entrada. Se o grupo de segurança tiver uma regra de entrada que abra portas para os endereços IP públicos IPv4 0.0.0.0/0 ou IPv6 ::/0, e essas portas não forem especificadas como exceções para a conta, o Amazon EMR não permitirá que o usuário crie o cluster.

> **Note**
>
> O bloqueio de acesso público é habilitado por padrão. Para aumentar a proteção da conta, é recomendável mantê-la habilitada.

Correção

Para configurar o bloqueio de acesso público para o Amazon EMR, consulte Uso do bloqueio de acesso público do Amazon EMR no Guia de gerenciamento do Amazon EMR.

Controles do Elasticsearch

Esses controles estão relacionados aos recursos do Elastic Beanstalk.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[ES.1] Os domínios do devem ter a criptografia em repouso habilitada.

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra do AWS Config : `elasticsearch-encrypted-at-rest`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se os domínios do têm a configuração da criptografia em repouso habilitada. Ocorrerá uma falha na verificação se a criptografia em repouso não estiver habilitada.

Para uma camada adicional de segurança para seus dados confidenciais OpenSearch, você deve configurá-los OpenSearch para serem criptografados em repouso. Os domínios do Elasticsearch oferecem criptografia de dados em repouso. O recurso é usado AWS KMS para armazenar e gerenciar suas chaves de criptografia. Para executar a criptografia, ele usa o algoritmo Advanced Encryption Standard com chaves de 256 bits (AES-256).

Para saber mais sobre OpenSearch criptografia em repouso, consulte Criptografia de dados em repouso para o Amazon OpenSearch Service no Amazon OpenSearch Service Developer Guide.

Certos tipos de instâncias não oferecem suporte à criptografia de dados em repouso. Para obter detalhes, consulte Tipos de instância compatíveis no Amazon OpenSearch Service Developer Guide.

Correção

Para habilitar a criptografia em repouso para domínios novos e existentes do Elasticsearch, consulte Habilitar a criptografia de dados em repouso no Amazon OpenSearch Service Developer Guide.

[ES.2] Os domínios do Elasticsearch não devem ser publicamente acessíveis

Requisitos relacionados: PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/1.3.2,PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

Categoria: Proteger > Configuração de rede segura

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `elasticsearch-in-vpc-only`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se os domínios do estão em uma VPC. Ele não avalia a configuração de roteamento da sub-rede da VPC para determinar a acessibilidade pública. Você deve garantir que os domínios do não estejam anexados a sub-redes públicas. Consulte as políticas baseadas em recursos no Amazon OpenSearch Service Developer Guide. Você também deve garantir que a VPC esteja configurada de acordo com as melhores práticas recomendadas. Para saber mais, consulte Grupos de segurança para a VPC no Manual do usuário do Amazon VPC.

Os domínios do Elasticsearch implantados em uma VPC podem se comunicar com os recursos da VPC pela rede AWS privada, sem a necessidade de atravessar a Internet pública. Essa configuração aumenta a postura de segurança ao limitar o acesso aos dados em trânsito. As VPCs fornecem vários controles de rede para proteger o acesso aos domínios do Elasticsearch, incluindo ACL de rede e grupos de segurança. O Security Hub recomenda que você migre domínios públicos do Elasticsearch para VPCs para aproveitar esses controles.

Correção

Se você criar um domínio com um endpoint público, não será possível colocá-lo em uma VPC posteriormente. Em vez disso, você deve criar um novo domínio e migrar seus dados. O inverso também é verdadeiro. Se você criar um domínio com uma VPC, ele não poderá ter um endpoint público. Em vez disso, você deve criar outro domínio ou desabilitar esse controle.

Consulte Lançamento de seus domínios do Amazon OpenSearch Service em uma VPC no OpenSearch Amazon Service Developer Guide.

Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em trânsito

Severidade: média

Tipo de recurso

Regra do AWS Config : `elasticsearch-node-to-node-encryption-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um domínio do Elasticsearch tem a node-to-node criptografia ativada. O controle falhará se o domínio Elasticsearch não tiver a node-to-node criptografia habilitada. O controle também produz descobertas malsucedidas se uma versão do Elasticsearch não oferecer suporte a verificações de node-to-node criptografia.

O HTTPS (TLS) pode ser usado para ajudar a impedir que possíveis invasores espionem ou manipulem o tráfego da rede usando ataques similares. person-in-the-middle Somente conexões criptografadas por HTTPS (TLS) devem ser permitidas. Habilitar a node-to-node criptografia para domínios do Elasticsearch garante que as comunicações entre clusters sejam criptografadas em trânsito.

Pode haver uma penalidade de desempenho associada a essa configuração. Você deve estar ciente e testar a compensação de desempenho antes de ativar essa opção.

Correção

Para obter informações sobre como habilitar a node-to-node criptografia em domínios novos e existentes, consulte Habilitar a node-to-node criptografia no Amazon OpenSearch Service Developer Guide.

[ES.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar – Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `elasticsearch-logs-to-cloudwatch`

Tipo de programação: acionado por alterações

Parâmetros:

- `logtype = 'error'` (não personalizável)

Esse controle verifica se os domínios do Elasticsearch estão configurados para enviar registros de erros para o Logs. CloudWatch

Você deve habilitar os registros de erros para os domínios do Elasticsearch e enviá-los aos Logs para CloudWatch retenção e resposta. Os logs de erros do domínio podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

Correção

Para obter informações sobre como habilitar a publicação de registros, consulte Habilitando a publicação de registros (console) no Amazon OpenSearch Service Developer Guide.

Os domínios do Elasticsearch devem ter o registro em log de auditoria ativado

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra AWS Config : `elasticsearch-audit-logging-enabled` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

- `cloudWatchLogsLogGroupArnList` (não personalizável). O Security Hub não preenche esse parâmetro. Lista separada por vírgulas de grupos de CloudWatch registros de registros que devem ser configurados para registros de auditoria.

  Essa regra é válida `NON_COMPLIANT` se o grupo de CloudWatch registros de registros do domínio Elasticsearch não estiver especificado nessa lista de parâmetros.

Esse controle verifica se os domínios do Elasticsearch têm o registro em log de auditoria ativado. Esse controle falhará se um domínio do Elasticsearch não tiver o registro em log de auditoria ativado.

Os registros em log de auditoria são altamente personalizáveis. Eles permitem que você acompanhe a atividade do usuário em seus clusters do Elasticsearch, incluindo sucessos e falhas de autenticação, solicitações, alterações de indexação e consultas de pesquisa recebidas. OpenSearch

Correção

Para obter instruções detalhadas sobre como habilitar registros de auditoria, consulte Habilitar registros de auditoria no Amazon OpenSearch Service Developer Guide.

Os domínios do Elasticsearch devem ter pelo menos três nós de dados

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra AWS Config : `elasticsearch-data-node-fault-tolerance` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os domínios do Elasticsearch estão configurados com pelo menos três nós de dados e `zoneAwarenessEnabled` é `true`.

Um domínio do Elasticsearch requer pelo menos três nós de dados para alta disponibilidade e tolerância a falhas. A implantação de um domínio do Elasticsearch com pelo menos três nós de dados garante as operações do cluster se um nó falhar.

Correção

Para modificar o número de nós de dados em um domínio do Elasticsearch

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/.

2. Em Domínios, escolha o nome do domínio que você deseja editar.
3. Selecione Edit domain (Editar domínio).
4. Em Nós de dados, defina Número de nós como um número maior ou igual a 3.

   Para três implantações de zona de disponibilidade, defina um múltiplo de três para garantir uma distribuição igual entre as zonas de disponibilidade.
5. Selecione Enviar.

Os domínios do Elasticsearch devem ser configurados com pelo menos três nós principais dedicados

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra AWS Config: `elasticsearch-primary-node-fault-tolerance` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os domínios do Elasticsearch estão configurados com pelo menos três nós primários dedicados. Esse controle falhará se o domínio não usar nós primários dedicados. Esse controle passa se os domínios do Elasticsearch tiverem cinco nós primários dedicados. No entanto, o uso de mais de três nós primários pode ser desnecessário para reduzir o risco de disponibilidade e resultará em custos adicionais.

Um domínio do Elasticsearch requer pelo menos três nós primários dedicados para alta disponibilidade e tolerância a falhas. Os recursos dedicados do nó primário podem ser sobrecarregados durante as implantações azul/verde do nó de dados porque há nós adicionais para gerenciar. A implantação de um domínio do Elasticsearch com pelo menos três nós primários dedicados garante capacidade suficiente de recursos do nó primário e operações de cluster se um nó falhar.

Correção

Para modificar o número de nós primários dedicados em um OpenSearch domínio

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/.
2. Em Domínios, escolha o nome do domínio que você deseja editar.
3. Selecione Edit domain (Editar domínio).
4. Em Nós principais dedicados, defina o Tipo de instância como o tipo de instância desejado.
5. Defina o Número de nós principais igual a três ou mais.
6. Selecione Enviar.

[ES.8] As conexões com os domínios do Elasticsearch devem ser criptografadas usando a política de segurança TLS mais recente

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em trânsito

Severidade: média

Tipo de recurso

Regra AWS Config : `elasticsearch-https-required` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Isso controla se um endpoint de domínio do Elasticsearch está configurado para usar a política de segurança TLS mais recente. O controle falhará se o endpoint do domínio Elasticsearch não estiver configurado para usar a política mais recente suportada ou se o HTTPs não estiver habilitado. A política de segurança TLS mais recente suportada atualmente é`Policy-Min-TLS-1-2-PFS-2023-10`.

O HTTPS (TLS) pode ser usado para ajudar a impedir que possíveis invasores usem ataques semelhantes para espionar person-in-the-middle ou manipular o tráfego da rede. Somente conexões

criptografadas por HTTPS (TLS) devem ser permitidas. A criptografia de dados em trânsito pode afetar o desempenho. Você deve testar seu aplicativo com esse atributo para entender o perfil de desempenho e o impacto do TLS. O TLS 1.2 fornece vários aprimoramentos de segurança em relação às versões anteriores do TLS.

Correção

Para ativar a criptografia TLS, use a operação UpdateDomainConfigda API para configurar o DomainEndpointOptionsobjeto. Isso define `TLSSecurityPolicy` o.

[ES.9] Os domínios do Elasticsearch devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-elasticsearch-domain` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um domínio do Elasticsearch tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o domínio não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro

`requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o domínio não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para [que serve o ABAC](#)? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como [marcar seus AWS recursos](#) no. Referência geral da AWS

Correção

Para adicionar tags a um domínio do Elasticsearch, consulte Como [trabalhar com tags](#) no Amazon OpenSearch Service Developer Guide.

EventBridge Controles da Amazon

Esses controles estão relacionados aos EventBridge recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte [Disponibilidade de controles por região](#).

[EventBridge.2] ônibus de EventBridge eventos devem ser etiquetados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

AWS Config regra: `tagged-events-eventbus` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um barramento de EventBridge eventos da Amazon tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o barramento de eventos não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o barramento de eventos não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM.

Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um ônibus de EventBridge eventos, consulte as EventBridge tags da Amazon no Guia EventBridge do usuário da Amazon.

[EventBridge.3] os ônibus de eventos EventBridge personalizados devem ter uma política baseada em recursos anexada

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Gerenciamento de acesso seguro > Configuração da política de recursos

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `custom-schema-registry-policy-attached`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um barramento de eventos EventBridge personalizado da Amazon tem uma política baseada em recursos anexada. Esse controle falhará se o barramento de eventos personalizado não tiver uma política baseada em recursos.

Por padrão, um barramento de eventos EventBridge personalizado não tem uma política baseada em recursos anexada. Isso permite que as entidades principais na conta acessem o barramento de eventos. Ao vincular uma política baseada em recursos ao barramento de eventos, é possível limitar

o acesso ao barramento de eventos a contas especificadas, bem como conceder acesso intencional a entidades em outra conta.

Correção

Para anexar uma política baseada em recursos a um barramento de eventos EventBridge personalizado, consulte Gerenciamento de permissões de barramento de eventos no Guia EventBridge do usuário da Amazon.

[EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra do AWS Config : `global-endpoint-event-replication-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se a replicação de eventos está habilitada para um endpoint EventBridge global da Amazon. O controle falhará se a replicação de eventos não estiver habilitada para um endpoint global.

Os endpoints globais ajudam a tornar seu aplicativo tolerante a falhas regionais. Para começar, você atribui uma verificação de integridade do Amazon Route 53 ao endpoint. Quando o failover é iniciado, a verificação de integridade relata um estado “não íntegro”. Poucos minutos após o início do failover, todos os eventos personalizados são roteados para um barramento de eventos na região secundária e processados por esse barramento de eventos. Ao usar endpoints globais, é possível ativar a replicação de eventos. A replicação de eventos envia todos os eventos personalizados para os barramentos de eventos nas regiões primária e secundária usando regras gerenciadas. Recomendamos ativar a replicação de eventos ao configurar endpoints globais. A replicação de eventos ajuda você a verificar se seus endpoints globais estão configurados corretamente. A replicação de eventos é necessária para se recuperar automaticamente de um evento de failover.

Se você não tiver a replicação de eventos ativada, precisará redefinir manualmente a verificação de integridade do Route 53 para “íntegra” antes que os eventos sejam redirecionados de volta para a região principal.

> **Note**
>
> Se você estiver usando um barramento de eventos personalizado, precisará de um barramento uniforme personalizado em cada região com o mesmo nome e na mesma conta para que o failover funcione corretamente. Habilitar a replicação de eventos pode aumentar seu custo mensal. Para obter informações sobre preços, consulte EventBridge Preços da Amazon.

Correção

Para habilitar a replicação de eventos para endpoints EventBridge globais, consulte Criar um endpoint global no Guia do usuário da Amazon EventBridge . Em Replicação de eventos, selecione Replicação de eventos ativada.

Controles do Amazon FSx

Esses controles estão relacionados aos recursos do Amazon FSx.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `fsx-openzfs-copy-tags-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um sistema de arquivos do Amazon FSx para OpenZFS está configurado para copiar tags para backups e volumes. O controle falhará se o sistema de arquivos OpenZFS não estiver configurado para copiar tags para backups e volumes.

A identificação e o inventário de seus ativos de TI é um aspecto importante de governança e segurança. As tags ajudam você a categorizar seus AWS recursos de maneiras diferentes, por exemplo, por finalidade, proprietário ou ambiente. Isso é útil quando você possui muitos recursos do mesmo tipo, pois torna possível identificar rapidamente um recurso específico baseado nas tags que você atribuiu a ele.

Correção

Para configurar um sistema de arquivos FSx for OpenZFS para copiar tags para backups e volumes, consulte Atualização de um sistema de arquivos no Guia do usuário do Amazon FSx OpenZFS.

[FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups

Requisitos relacionados: NIST.800-53.r5 CP-9, NIST.800-53.r5 CM-8

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `fsx-lustre-copy-tags-to-backups`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um sistema de arquivos Amazon FSx for Lustre está configurado para copiar tags para backups e volumes. O controle falhará se o sistema de arquivos Lustre não estiver configurado para copiar tags para backups e volumes.

A identificação e o inventário de seus ativos de TI é um aspecto importante de governança e segurança. As tags ajudam você a categorizar seus AWS recursos de maneiras diferentes, por exemplo, por finalidade, proprietário ou ambiente. Isso é útil quando você possui muitos recursos do mesmo tipo, pois torna possível identificar rapidamente um recurso específico baseado nas tags que você atribuiu a ele.

Correção

Para configurar um sistema de arquivos FSx for Lustre para copiar tags para backups, consulte Atualização de um sistema de arquivos no Guia do usuário do Amazon FSx OpenZFS.

AWS Global Accelerator controles

Esses controles estão relacionados aos recursos do Global Accelerator.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-globalaccelerator-accelerator` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um AWS Global Accelerator acelerador tem tags com as teclas específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o acelerador não tiver nenhuma

chave de tag ou se não tiver todas as teclas especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o acelerador não estiver marcado com nenhuma tecla. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um acelerador global do Global Accelerator, consulte Como inserir tags AWS Global Accelerator no Guia do AWS Global Accelerator desenvolvedor.

AWS Glue controles

Esses controles estão relacionados aos AWS Glue recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

Os AWS Glue trabalhos [Glue.1] devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

AWS Config regra: `tagged-glue-job` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um AWS Glue trabalho tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o trabalho não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o trabalho não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder

à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um AWS Glue trabalho, consulte as AWS tags AWS Glue no Guia do AWS Glue usuário.

GuardDuty Controles da Amazon

Esses controles estão relacionados aos GuardDuty recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[GuardDuty.1] GuardDuty deve ser ativado

Requisitos relacionados: PCI DSS v3.2.1/11.4, NIST.800-53.r5 AC-2(12), NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(5), NIST.800-53.r5 CA-7, NIST.800-53.r5 CM-8(3), NIST.800-53.r5 RA-3(4), NIST.800-53.r5 SA-11(1), NIST.800-53.r5 SA-11(6), NIST.800-53.r5 SA-15(2), NIST.800-53.r5 SA-15(8), NIST.800-53.r5 SA-8(19), NIST.800-53.r5 SA-8(21), NIST.800-53.r5 SA-8(25), NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-5(1), NIST.800-53.r5 SC-5(3), NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4(1), NIST.800-53.r5 SI-4(13), NIST.800-53.r5 SI-4(2), NIST.800-53.r5 SI-4(22), NIST.800-53.r5 SI-4(25), NIST.800-53.r5 SI-4(4), NIST.800-53.r5 SI-4(5)

Categoria: Detectar > Serviços de detecção

Severidade: alta

Tipo de recurso

Regra do AWS Config : `guardduty-enabled-centralized`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se a Amazon GuardDuty está habilitada em sua GuardDuty conta e região.

É altamente recomendável que você habilite GuardDuty em todas as AWS regiões suportadas. Isso permite GuardDuty gerar descobertas sobre atividades não autorizadas ou incomuns, mesmo em regiões que você não usa ativamente. Isso também permite GuardDuty monitorar CloudTrail eventos globais Serviços da AWS , como o IAM.

Correção

Para corrigir esse problema, você ativa GuardDuty.

Para obter detalhes sobre como habilitar GuardDuty, incluindo como usar AWS Organizations para gerenciar várias contas, consulte Getting Started with GuardDuty no Guia GuardDuty do usuário da Amazon.

[GuardDuty.2] GuardDuty os filtros devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-guardduty-filter` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o	StringList	Lista de tags que atendem	`No default value`

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.		aos AWS requisitos	

Esse controle verifica se um GuardDuty filtro da Amazon tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o filtro não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o filtro não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um GuardDuty filtro, consulte TagResourcena Amazon GuardDuty API Reference.

[GuardDuty.3] Os GuardDuty IPsets devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-guardduty-ipset` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um Amazon GuardDuty IPSet tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o IPSet não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o IPSet não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou

outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um GuardDuty IPSet, consulte TagResourcena Amazon GuardDuty API Reference.

[GuardDuty.4] os GuardDuty detectores devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-guardduty-detector` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um GuardDuty detector da Amazon tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o detector não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle verificará apenas a existência de uma chave de tag e falhará se o detector não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS

Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um GuardDuty detector, consulte TagResourcena Amazon GuardDuty API Reference.

AWS Identity and Access Management controles

Esses controles estão relacionados aos recursos do IAM.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[IAM.1] As políticas do não devem permitir privilégios administrativos completos "*"

Requisitos relacionados: PCI DSS v3.2.1/7.2.1, CIS Foundations Benchmark v1.2.0/1.22, CIS AWS Foundations Benchmark v1.4.0/1.16, NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 3.r5 AC-3 (7), Nist.800-53.R5 AC-5, Nist.800-53.R5 AC-6, Nist.800-53.R5 AC-6 (10), Nist.800-53.R5 AC-6 (2), Nist.800-53.R5 AC-6 (3) AWS

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: alta

Tipo de recurso

Regra do AWS Config : `iam-policy-no-statements-with-admin-access`

Tipo de programação: acionado por alterações

Parâmetros:

- `excludePermissionBoundaryPolicy: true` (não personalizável)

Esse controle verifica se a versão padrão das políticas do IAM (também conhecidas como políticas gerenciadas pelo cliente) não tem acesso de administrador com uma instrução que

tenha`"Effect": "Allow"` com `"Action": "*"` em `"Resource": "*"`. O controle falhará se você tiver políticas do IAM com essa declaração.

O controle apenas verifica as políticas gerenciadas pelo cliente que você criou. Ele não verifica políticas em linha e AWS gerenciadas.

As políticas do definem um conjunto de privilégios concedidos a usuários, grupos ou funções. Seguindo o conselho de segurança padrão, AWS recomenda que você conceda privilégios mínimos, o que significa conceder somente as permissões necessárias para realizar uma tarefa. Ao fornecer privilégios administrativos completos em vez do conjunto mínimo de permissões que o usuário precisa, você expõe os recursos a ações potencialmente indesejadas.

Em vez de permitir privilégios administrativos completos, determine o que os usuários precisam fazer e crie políticas que permitam que executem apenas aquelas tarefas. É mais seguro começar com um conjunto mínimo de permissões e conceder permissões adicionais conforme necessário. Não comece com permissões que sejam muito flexíveis para depois tentar restringi-las.

Remova as políticas do IAM `"Effect": "Allow"` que têm uma instrução com `"Action": "*"` por `"Resource": "*"`.

> **Note**
>
> AWS Config deve estar habilitado em todas as regiões nas quais você usa o Security Hub. Entretanto, a gravação global de recursos pode ser ativada em uma única região. Se você registrar apenas recursos globais em uma única região, poderá desabilitar esse controle em todas as regiões, exceto na região em que registra recursos globais.

Correção

Para modificar suas políticas do IAM para que elas não permitam privilégios administrativos “*” completos, consulte Editar políticas do IAM no Guia do usuário do IAM.

[IAM.2] Os usuários do não devem ter políticas do IAM anexadas

Requisitos relacionados: PCI DSS v3.2.1/7.2.1, CIS Foundations Benchmark v3.0.0/1.15, CIS AWS Foundations Benchmark v1.2.0/1.16, NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 3.r5 AC-3 (7), Nist.800-53.R5 AC-6, Nist.800-53.R5 AC-6 (3) AWS

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `iam-user-no-policies-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se nenhum dos usuários do IAM tem políticas anexadas. O controle falhará se seus usuários do IAM tiverem políticas vinculadas. Em vez disso, os usuários do IAM devem herdar permissões dos grupos ou funções do .

Por padrão, usuários, grupos e funções do IAM não têm acesso aos AWS recursos. As políticas do IAM são como os privilégios são concedidos aos usuários, aos grupos ou às funções na . Recomendamos que você aplique as políticas do IAM diretamente a grupos e funções, mas não aos usuários. A atribuição de privilégios no nível do grupo ou função reduz a complexidade do gerenciamento de acesso à medida que o número de usuários aumenta. Reduzir a complexidade do gerenciamento de acesso pode, por sua vez, reduzir a oportunidade para uma entidade principal inadvertidamente receber ou manter um número excessivo de privilégios.

> **Note**
>
> Os usuários do IAM criados pelo Amazon Simple Email Service são criados automaticamente usando políticas em linha. O Security Hub isenta automaticamente esses usuários desse controle.
> AWS Config deve estar habilitado em todas as regiões nas quais você usa o Security Hub. Entretanto, a gravação global de recursos pode ser ativada em uma única região. Se você registrar apenas recursos globais em uma única região, poderá desabilitar esse controle em todas as regiões, exceto na região em que registra recursos globais.

Correção

Para resolver esse problema, crie um grupo do IAM e anexe a política ao grupo. Adicione os usuários ao grupo A política é aplicada a cada usuário no grupo. Para remover uma política vinculada diretamente a um usuário, consulte Adicionar e remover permissões de identidade do IAM no Guia do usuário do IAM.

[IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/1.14, CIS Foundations Benchmark v1.4.0/1.14, CIS AWS Foundations Benchmark v1.2.0/1.4, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-2 (3), AWS NIST.800-53.r5 AC-3 (15)

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `access-keys-rotated`

Tipo de programação: Periódico

Parâmetros:

- `maxAccessKeyAge`: `90` (não personalizável)

Esse controle verifica se as chaves de acesso ativas são mudadas em até 90 dias.

É altamente recomendado não gerar e remover todas as chaves de acesso na conta. Em vez disso, a melhor prática recomendada é criar uma ou mais funções do IAM ou usar a federação por meio de AWS IAM Identity Center. Você pode usar esses métodos para permitir que seus usuários acessem AWS Management Console AWS CLI e.

Cada abordagem tem os respectivos casos de uso. A federação é geralmente melhor para empresas com um diretório central existente ou que projetam a necessidade de um número maior do que o limite atual de usuários do . Os aplicativos executados fora de um AWS ambiente precisam de chaves de acesso para acesso programático aos AWS recursos.

No entanto, se os recursos que precisam de acesso programático forem executados internamente AWS, a melhor prática é usar funções do IAM. As funções permitem conceder acesso a recursos sem codificar um ID de chave de acesso e uma chave de acesso secreta na configuração.

Para saber mais sobre como proteger suas chaves de acesso e sua conta, consulte Melhores práticas para gerenciar chaves de AWS acesso no Referência geral da AWS. Veja também a postagem do blog Diretrizes para proteger você Conta da AWS ao usar o acesso programático.

Caso já tenha uma chave de acesso, o recomenda mudar as chaves de acesso a cada 90 dias. A mudança de chaves de acesso reduz a chance de uso de uma chave de acesso associada a uma conta comprometida ou encerrada. Isso também garante que os dados não possam ser acessados com uma chave antiga que pode ter sido perdida, decifrada ou roubada. Sempre atualize os aplicativos após mudar as chaves de acesso.

As chaves de acesso consistem em um ID de chave de acesso e em uma chave de acesso secreta. Elas são usadas para assinar as solicitações programáticas que você faz à AWS. Os usuários precisam de suas próprias chaves de acesso para fazer chamadas programáticas a AWS partir do AWS CLI Tools for Windows PowerShell, dos AWS SDKs ou chamadas HTTP diretas usando as operações de API individuais. Serviços da AWS

Se sua organização usa AWS IAM Identity Center (IAM Identity Center), seus usuários podem entrar no Active Directory, em um diretório integrado do IAM Identity Center ou em outro provedor de identidade (IdP) conectado ao IAM Identity Center. Em seguida, eles podem ser mapeados para uma função do IAM que permite executar AWS CLI comandos ou chamar operações de AWS API sem a necessidade de chaves de acesso. Para saber mais, consulte Configurando o AWS CLI para uso AWS IAM Identity Center no Guia do AWS Command Line Interface usuário.

> **Note**
>
> AWS Config deve estar habilitado em todas as regiões nas quais você usa o Security Hub. Entretanto, a gravação global de recursos pode ser ativada em uma única região. Se você registrar apenas recursos globais em uma única região, poderá desabilitar esse controle em todas as regiões, exceto na região em que registra recursos globais.

Correção

Para alternar chaves de acesso com mais de 90 dias, consulte Chaves de acesso rotativas no Guia do usuário do IAM. Siga as instruções para qualquer usuário com uma chave de acesso com idade superior a 90 dias.

[IAM.4] A chave de acesso do usuário raiz do não deve existir

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/1.4, CIS Foundations Benchmark v1.4.0/1.4, CIS AWS Foundations Benchmark v1.2.0/1.12, PCI DSS v3.2.1/2.1, PCI DSS v3.2.1/2.2, AWS PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15)), Nist.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-6, Nist.800-53.r5 AC-6 (10), Nist.800-53.R5 AC-6 (2)

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `iam-root-access-key-check`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se a chave de acesso do usuário raiz está disponível.

O usuário root é o usuário mais privilegiado em um Conta da AWS. AWS as teclas de acesso fornecem acesso programático a uma determinada conta.

O recomenda remover todas as chaves de acesso associadas à conta raiz. Isso limita os vetores que podem ser usados para comprometer a conta. Além disso, incentiva a criação e o uso de contas baseadas em função que são menos privilegiadas.

Correção

Para excluir a chave de acesso do usuário raiz, consulte Excluir chaves de acesso para o usuário raiz no Guia do usuário do IAM. Para excluir as chaves de acesso do usuário root de um Conta da AWS in AWS GovCloud (US), consulte Excluindo as chaves de acesso do usuário raiz da minha AWS GovCloud (US) conta no Guia do AWS GovCloud (US) usuário.

[IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/1.10, CIS Foundations Benchmark v1.4.0/1.10, CIS AWS Foundations Benchmark v1.2.0/1.2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), NIST.800-53.r5 IA-2 (2)), Nist.800-53.r5 IA-2 (6), Nist.800-53.r5 IA-2 (8) AWS

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `mfa-enabled-for-iam-console-access`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se a autenticação AWS multifator (MFA) está habilitada para todos os usuários do IAM que usam uma senha de console.

A autenticação multifator (MFA) adiciona uma camada extra de proteção sobre um nome de usuário e senha. Com o MFA ativado, quando um usuário faz login em um AWS site, ele é solicitado a fornecer seu nome de usuário e senha. Além disso, eles são solicitados a fornecer um código de autenticação de seu dispositivo de AWS MFA.

Recomendamos habilitar a MFA para todas as contas que têm uma senha do console. A MFA foi projetada para fornecer maior segurança para o acesso ao console. O principal de autenticação deve conter um dispositivo que emite uma chave sensível ao tempo e deve ter conhecimento de uma credencial.

> **Note**
>
> AWS Config deve estar habilitado em todas as regiões nas quais você usa o Security Hub. Entretanto, a gravação global de recursos pode ser ativada em uma única região. Se você registrar apenas recursos globais em uma única região, poderá desabilitar esse controle em todas as regiões, exceto na região em que registra recursos globais.

Correção

Para saber mais, consulte Usar autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

Estamos oferecendo uma chave de segurança de MFA gratuita para clientes qualificados. Veja se você se qualifica e solicite sua chave gratuita.

[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/1.6, CIS Foundations Benchmark v1.4.0/1.6, CIS AWS Foundations Benchmark v1.2.0/1.14, PCI DSS v3.2.1/8.3.1, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), NIST.800-53.r5 800-53.r5 IA-2 (2), Nist.800-53.R5 IA-2 (6), NISt.800-53.r5 IA-2 (8) AWS

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `root-account-hardware-mfa-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se você Conta da AWS está habilitado para usar um dispositivo de autenticação multifator (MFA) de hardware para fazer login com credenciais de usuário raiz. O controle falhará se a MFA não estiver habilitada ou se algum dispositivo virtual de MFA tiver permissão para fazer login com credenciais de usuário raiz.

A MFA virtual pode não fornecer o mesmo nível de segurança oferecido por dispositivos MFA de hardware. Recomendamos usar um dispositivo MFA virtual somente enquanto aguarda a aprovação da compra do hardware ou a chegada do hardware. Para saber mais, consulte Habilitar um dispositivo Multi-Factor Authentication (MFA) (console) no IAM.

Tanto os tokens de senha de uso único com marcação temporal (TOTP) quanto os tokens do Universal 2nd Factor (U2F) são viáveis como opções de MFA de hardware.

Correção

Para adicionar um dispositivo de MFA de hardware para o usuário raiz, consulte Habilitar um dispositivo de MFA de hardware para o usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Estamos oferecendo uma chave de segurança de MFA gratuita para clientes qualificados. Veja se você se qualifica e solicite sua chave gratuita.

[IAM.7] As políticas de senha para usuários do IAM devem ter configurações fortes

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `iam-password-policy`

Tipo de programação: Periódico

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`RequireUppercaseCharacters`	Exige pelo menos um caractere maiúsculo na senha	Booleano	`true` ou `false`	`true`
`RequireLowercaseCharacters`	Exige pelo menos um caractere minúsculo na senha	Booleano	`true` ou `false`	`true`
`RequireSymbols`	Exige pelo menos um símbolo na senha	Booleano	`true` ou `false`	`true`
`RequireNumbers`	Exige pelo menos um número na senha	Booleano	`true` ou `false`	`true`
`MinimumPasswordLength`	Número mínimo de caracteres na senha	Inteiro	8 para 128	8
`PasswordReusePrevention`	Número de rotações de senha antes que uma senha antiga possa ser reutilizada	Inteiro	12 para 24	Nenhum valor padrão
`MaxPasswordAge`	Número de dias antes da expiração da senha	Inteiro	1 para 90	Nenhum valor padrão

Esse controle verifica se a política de senha de conta para usuários do IAM usa configurações fortes. O controle falhará se a política de senha não usar configurações fortes. A menos que você forneça valores de parâmetros personalizados, o Security Hub usará os valores padrão mencionados na tabela anterior. Os parâmetros `PasswordReusePrevention` e `MaxPasswordAge` não têm valor padrão, portanto, se você excluir esses parâmetros, o Security Hub ignorará o número de rotações da senha e a idade da senha ao avaliar esse controle.

Para acessar o AWS Management Console, os usuários do IAM precisam de senhas. Como prática recomendada, o Security Hub recomenda enfaticamente que, em vez de criar usuários do IAM, você use a federação. A federação permite que os usuários usem suas credenciais corporativas existentes para fazer login no AWS Management Console. Use AWS IAM Identity Center (IAM Identity Center) para criar ou federar o usuário e, em seguida, assumir uma função do IAM em uma conta.

Para saber mais sobre provedores de identidade e federação, consulte Provedores de identidade e federação no Guia do usuário do IAM. Para saber mais sobre o Centro de Identidade do IAM, consulte .

Se você precisar usar usuários do IAM, o Security Hub recomenda que você imponha a criação de senhas de usuário fortes. Você pode definir uma política de senha Conta da AWS para especificar requisitos de complexidade e períodos de rotação obrigatórios para senhas. Quando você criar ou alterar uma política de senha, a maioria das configurações de política de senha será aplicada da próxima vez que seus usuários mudarem suas senhas. Entretanto, algumas das configurações serão aplicadas imediatamente.

Correção

Para atualizar sua política de senha, consulte Configuração de uma política de senha de conta para usuários do IAM no Guia do usuário do IAM.

As credenciais de usuário do IAM não utilizadas devem ser removidas

Requisitos relacionados: PCI DSS v3.2.1/8.1.4, CIS AWS Foundations Benchmark v1.2.0/1.3, NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-2 (3), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 -53,5R5 AC-3 (7), Nist.800-53,5R5 AC-6

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `iam-user-unused-credentials-check`

Tipo de programação: Periódico

Parâmetros:

- `maxCredentialUsageAge`: `90` (não personalizável)

Esse controle verifica se seus usuários do IAM têm senhas ou chaves de acesso ativas que não foram usadas por 90 dias.

Os usuários do IAM podem acessar AWS recursos usando diferentes tipos de credenciais, como senhas ou chaves de acesso.

Recomendamos que você remova ou desative todas as credenciais que não foram usadas em 90 dias ou mais. Desabilitar ou remover credenciais desnecessárias reduz a possibilidade de uso de credenciais associadas a uma conta comprometida ou abandonada.

> **Note**
>
> AWS Config deve estar habilitado em todas as regiões nas quais você usa o Security Hub. Entretanto, a gravação global de recursos pode ser ativada em uma única região. Se você registrar apenas recursos globais em uma única região, poderá desabilitar esse controle em todas as regiões, exceto na região em que registra recursos globais.

Correção

Quando você visualiza as informações do usuário no console do IAM, há colunas para Idade da chave de acesso, Idade da senha e Última atividade. Se o valor em qualquer uma dessas colunas for maior do que 90 dias, deixe as credenciais para esses usuários inativas.

Você também pode usar os relatórios de credenciais para monitorar e identificar as contas de usuário sem atividade por 90 dias ou mais. É possível baixar os relatórios de credenciais no formato .csv no console do IAM `.csv`.

Depois de identificar as contas inativas ou as credenciais não utilizadas, desative-as. Para instruções, consulte Criar, alterar ou excluir uma senha de usuário do IAM (console) no Guia do usuário do IAM.

[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz

Requisitos relacionados: PCI DSS v3.2.1/8.3.1, CIS Foundations Benchmark v3.0.0/1.5, CIS Foundations Benchmark v1.4.0/1.5, CIS AWS Foundations Benchmark v1.2.0/1.13, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), NIST.800-53.r5 800-53.r5 IA-2 (2), Nist.800-53.R5 IA-2 (6), NISt.800-53.r5 IA-2 (8) AWS AWS

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `root-account-mfa-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

O usuário raiz tem acesso a todos os serviços e recursos da Conta da AWS na conta. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Com o MFA ativado, quando um usuário faz login no AWS Management Console, ele é solicitado a fornecer seu nome de usuário e senha e um código de autenticação de seu dispositivo de AWS MFA.

Ao usar MFA virtual para contas raiz, o recomenda que o dispositivo usado não seja um dispositivo pessoal. Em vez disso, use um dispositivo móvel dedicado (tablet ou telefone) que você gerencia para manter carregado e seguro independente dos dispositivos pessoais individuais. Isso reduz o risco de perder o acesso ao dispositivo MFA devido a perda ou negociação de dispositivo ou se o proprietário do dispositivo não estiver mais empregado na empresa.

Correção

Para habilitar o MFA para o usuário raiz, consulte Ativar o MFA no usuário Conta da AWS raiz no Guia de referência de gerenciamento de AWS contas.

[IAM.10] As políticas de senha para usuários do IAM devem ter durações fortes AWS Config

Requisitos relacionados: PCI DSS v3.2.1/8.1.4, PCI DSS v3.2.1/8.2.3, PCI DSS v3.2.1/8.2.4, PCI DSS v3.2.1/8.2.5

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `iam-password-policy`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se a política da senha da conta para usuários do IAM usa as configurações recomendadas a seguir.

- Exige pelo menos um caractere maiúsculo na senha. (Padrão = `true`)
- Exige pelo menos um caractere minúsculo na senha. (Padrão = `true`)
- Exige pelo menos um número na senha. (Padrão = `true`)
- Tamanho mínimo da senha. (Padrão = 7 ou mais)
- Número de senhas antes de permitir a reutilização. Padrão: 4 ()
- MaxPasswordAge — Número de dias antes da expiração da senha. (Padrão = 0)

Correção

Para atualizar sua política de senha para usar a configuração recomendada, consulte Como definir uma política de senha de conta para usuários do IAM no Guia do usuário do IAM.

1.5 Certifique-se de que política de senha do IAM exija pelo menos uma letra maiúscula

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/1.5

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `iam-password-policy`

Tipo de programação: Periódico

Parâmetros: nenhum

As políticas de senha, em parte, impõem requisitos de complexidade de senha. Use políticas de senha do IAM para garantir que as senhas usem diferentes conjuntos de caracteres.

Recomendamos que a política de senhas exija pelo menos uma letra maiúscula. Definir uma política de complexidade de senha aumenta a resiliência da conta contra tentativas de login forçado.

Correção

Para atualizar sua política de senha para usar a configuração recomendada, consulte Como definir uma política de senha de conta para usuários do IAM no Guia do usuário do IAM. Exigir pelo menos uma letra maiúscula do alfabeto latino (A–Z)

1.6 Certifique-se de que política de senha do IAM exija pelo menos uma letra minúscula

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/1.6

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `iam-password-policy`

Tipo de programação: Periódico

Parâmetros: nenhum

As políticas de senha, em parte, impõem requisitos de complexidade de senha. Use políticas de senha do IAM para garantir que as senhas usem diferentes conjuntos de caracteres. Recomendamos que a política de senhas exija pelo menos uma letra minúscula. Definir uma política de complexidade de senha aumenta a resiliência da conta contra tentativas de login forçado.

Correção

Para atualizar sua política de senha para usar a configuração recomendada, consulte Como definir uma política de senha de conta para usuários do IAM no Guia do usuário do IAM. Exigir pelo menos uma letra minúscula do alfabeto latino (a–z)

1.7 Certifique-se de que política de senha do IAM exija pelo menos um símbolo

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/1.7

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `iam-password-policy`

Tipo de programação: Periódico

Parâmetros: nenhum

As políticas de senha, em parte, impõem requisitos de complexidade de senha. Use políticas de senha do IAM para garantir que as senhas usem diferentes conjuntos de caracteres.

Recomendamos que a política de senhas exija pelo menos um símbolo. Definir uma política de complexidade de senha aumenta a resiliência da conta contra tentativas de login forçado.

Correção

Para atualizar sua política de senha para usar a configuração recomendada, consulte Como definir uma política de senha de conta para usuários do IAM no Guia do usuário do IAM. Em Força da senha, selecione Exigir pelo menos um caractere não alfanumérico.

Certifique-se de que política de senha do IAM exija pelo menos um número

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/1.8

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `iam-password-policy`

Tipo de programação: Periódico

Parâmetros: nenhum

As políticas de senha, em parte, impõem requisitos de complexidade de senha. Use políticas de senha do IAM para garantir que as senhas usem diferentes conjuntos de caracteres.

Recomendamos que a política de senhas exija pelo menos um número. Definir uma política de complexidade de senha aumenta a resiliência da conta contra tentativas de login forçado.

Correção

Para atualizar sua política de senha para usar a configuração recomendada, consulte Como definir uma política de senha de conta para usuários do IAM no Guia do usuário do IAM. Em Força da senha, selecione Exigir pelo menos um caractere não alfanumérico.

1.9 Certifique-se de que a política de senha do IAM exija um comprimento mínimo de 14 ou mais

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/1.8, CIS Foundations Benchmark v1.4.0/1.8, CIS AWS Foundations Benchmark v1.2.0/1.9 AWS

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `iam-password-policy`

Tipo de programação: Periódico

Parâmetros: nenhum

As políticas de senha, em parte, impõem requisitos de complexidade de senha. Use políticas de senha do para garantir que as senhas tenham pelo menos um determinado comprimento.

Recomendamos que a política de senha exija um comprimento mínimo para senha de 14 caracteres. Definir uma política de complexidade de senha aumenta a resiliência da conta contra tentativas de login forçado.

Correção

Para atualizar sua política de senha para usar a configuração recomendada, consulte Como definir uma política de senha de conta para usuários do IAM no Guia do usuário do IAM. Em Tamanho mínimo da senha, insira **14** ou um número maior.

1.10 Certifique-se de que a política de senha do IAM impeça a reutilização de senhas

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/1.9, CIS Foundations Benchmark v1.4.0/1.9, CIS AWS Foundations Benchmark v1.2.0/1.10 AWS

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `iam-password-policy`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o número de senhas a serem lembradas está definido como 24. O controle falhará se o valor não for 24.

As políticas de senha do podem impedir a reutilização de uma determinada senha pelo mesmo usuário.

Recomendamos que a política de senha impeça a reutilização de senhas. Impedir a reutilização de senhas aumenta a resiliência da conta contra tentativas de login forçado.

Correção

Para atualizar sua política de senha para usar a configuração recomendada, consulte Como definir uma política de senha de conta para usuários do IAM no Guia do usuário do IAM. Em Impedir a reutilização da senha, digite **24**.

1.11 Certifique-se de que a política de senha do IAM expire senhas em até 90 dias ou menos

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/1.11

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `iam-password-policy`

Tipo de programação: Periódico

Parâmetros: nenhum

As políticas de senha do podem exigir a mudança ou expiração de senhas após um determinado número de dias.

Recomendamos que a política de senha expire senhas após 90 dias ou menos. Reduzir a duração da senha aumenta a resiliência da conta contra tentativas de login forçado. Exigir alterações de senha regulares ajuda nos seguintes cenários:

- As senhas podem ser roubadas ou comprometidas sem o seu conhecimento. Isso pode acontecer por meio de um comprometimento do sistema, vulnerabilidade de software ou ameaças internas.
- Alguns filtros governamentais e corporativos da Web ou servidores de proxy podem interceptar e registrar o tráfego mesmo se ele for criptografado.
- Muitas pessoas usam a mesma senha para muitos sistemas, como trabalho, email e pessoal.
- Estações de trabalho do usuário final comprometidas podem ter um registrador de teclas.

Correção

Para atualizar sua política de senha para usar a configuração recomendada, consulte Como definir uma política de senha de conta para usuários do IAM no Guia do usuário do IAM. Em Ativar a expiração da senha, digite **`90`** ou um número menor.

[IAM.18] Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support

Requisitos relacionados: CIS Foundations Benchmark v3.0.0/1.17, CIS AWS Foundations Benchmark v1.4.0/1.17, CIS AWS Foundations Benchmark v1.2.0/1.20 AWS

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `iam-policy-in-use`

Tipo de programação: Periódico

Parâmetros:

- `policyARN`: `arn:partition:iam::aws:policy/AWSSupportAccess` (não personalizável)
- `policyUsageType`: `ANY` (não personalizável)

AWS fornece um centro de suporte que pode ser usado para notificação e resposta a incidentes, bem como suporte técnico e atendimento ao cliente.

Crie uma função do para permitir que usuários autorizados gerenciem incidentes com o Support. Ao implementar o menor privilégio para controle de acesso, uma função do IAM exigirá uma política de IAM apropriada para permitir o acesso ao centro de suporte a fim de gerenciar incidentes com. AWS Support

> **Note**
>
> AWS Config deve estar habilitado em todas as regiões nas quais você usa o Security Hub. Entretanto, a gravação global de recursos pode ser ativada em uma única região. Se você registrar apenas recursos globais em uma única região, poderá desabilitar esse controle em todas as regiões, exceto na região em que registra recursos globais.

Correção

Para corrigir esse problema, crie uma função para permitir que usuários autorizados gerenciem incidentes do AWS Support Support.

Para criar a função a ser usada para AWS Support acesso

1. Abra o console IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Perfis e escolha Criar perfil.
3. Em Role type (Tipo de função), escolha Another AWS account (Outra conta da AWS) Conta da AWS.
4. Em ID da conta, insira Conta da AWS a Conta da AWS ID da qual você deseja conceder acesso aos seus recursos.

Se os usuários ou grupos que assumirão essa função estiverem na mesma conta, insira o número da conta local.

> **Note**
>
> O administrador da conta especificada pode conceder permissão para assumir essa função a qualquer usuário do . Para fazer isso, o administrador anexa uma política ao usuário ou grupo que concede permissão para a ação `sts:AssumeRole`. Nessa política, o recurso deve ser o ARN da função.

5. Escolha Próximo: permissões.
6. Procure a política gerenciada `AWSSupportAccess`.
7. Marque a caixa de seleção da política gerenciada `AWSSupportAccess`.
8. Escolha Próximo: etiquetas.
9. (Opcional) Para adicionar metadados à função, anexe tags como pares de chave-valor.

   Para obter mais informações sobre o uso de tags no IAM, consulte Marcar usuários e funções do IAM no Guia do usuário do IAM.
10. Selecione Next: Review (Próximo: revisar).
11. Em Role name (Nome da função), digite um nome para sua função.

    Os nomes das funções devem ser exclusivos em seu Conta da AWS. Não diferenciam letras maiúsculas de minúsculas.
12. (Opcional) Em Descrição da função, insira uma descrição para o novo perfil.
13. Revise a função e selecione Create role (Criar função).

[PCI.IAM.6] A MFA deve estar habilitada para todos os usuários do

Requisitos relacionados: CIS Foundations Benchmark v1.2.0/1.2, CIS Foundations Benchmark v1.4.0/1.10, NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3(15), NIST.800-53.r5 IA-2(1), NIST.800-53.r5 IA-2(2), NIST.800-53.r5 IA-2(6), NIST.800-53.r5 IA-2(8)

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `iam-user-mfa-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se os usuários do têm a autenticação multifator (MFA) habilitada.

> **Note**
>
> AWS Config deve estar habilitado em todas as regiões nas quais você usa o Security Hub. Entretanto, a gravação global de recursos pode ser ativada em uma única região. Se você registrar apenas recursos globais em uma única região, poderá desabilitar esse controle em todas as regiões, exceto na região em que registra recursos globais.

Correção

Para adicionar MFA para usuários do IAM, consulte Habilitar dispositivos de MFA para usuários na AWS no Guia do usuário do IAM.

Evitar o uso do usuário raiz

> **Important**
>
> O Security Hub retirou esse controle em abril de 2024. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Requisitos relacionados: CIS AWS Foundations Benchmark v1.2.0/1.1

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: baixa

Tipo de recurso

Regra AWS Config : `use-of-root-account-test` (regra personalizada do Security Hub)

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um Conta da AWS tem restrições ao uso do usuário root. O controle avalia os seguintes recursos:

- Amazon Simple Notification Service (Amazon SNS) topics
- AWS CloudTrail trilhas
- Filtros métricos associados às CloudTrail trilhas
- CloudWatch Alarmes da Amazon com base nos filtros

Essa verificação resulta em uma descoberta `FAILED` se uma ou mais das seguintes afirmações são verdadeiras:

- Não existem CloudTrail trilhas na conta.
- Uma CloudTrail trilha está ativada, mas não está configurada com pelo menos uma trilha multirregional que inclui eventos de gerenciamento de leitura e gravação.
- Uma CloudTrail trilha está ativada, mas não está associada a um grupo de CloudWatch registros de registros.
- O filtro métrico exato prescrito pelo Center for Internet Security (CIS) não é usado. O filtro métrico prescrito é `'{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}'`.
- Não há CloudWatch alarmes baseados no filtro métrico na conta.
- CloudWatch os alarmes configurados para enviar notificação ao tópico SNS associado não são acionados com base na condição do alarme.
- O tópico do SNS não está em conformidade com as restrições de envio de uma mensagem para um tópico do SNS.
- O tópico do SNS não tem pelo menos um assinante.

Essa verificação resulta em uma descoberta `NO_DATA` se uma ou mais das seguintes afirmações são verdadeiras:

- As trilhas multirregionais também podem ser baseadas em uma região diferente. O Security Hub só pode gerar descobertas na região em que a trilha está baseada.
- Uma trilha multirregional pertence a uma conta diferente. O Security Hub só pode gerar descobertas para a conta proprietária da trilha.

Essa verificação resulta em uma descoberta `WARNING` se uma ou mais das seguintes afirmações são verdadeiras:

- A conta atual não é proprietária do tópico SNS referenciado no CloudWatch alarme.
- A conta atual não tem acesso ao tópico do SNS ao invocar a API do SNS `ListSubscriptionsByTopic`.

> **Note**
>
> Recomendamos trilhas organizacionais para registrar eventos de logs de várias contas em uma organização. Por padrão, as trilhas da organização são trilhas multirregionais e só podem ser gerenciadas pela conta AWS Organizations de gerenciamento ou pela conta de administrador CloudTrail delegado. O uso de uma trilha organizacional resulta em um status de controle de aos controles avaliados nas contas dos membros da organização. Nas contas dos membros, o Security Hub só gera descobertas para recursos de propriedade dos membros. As descobertas relacionadas às trilhas da organização são geradas na conta do proprietário do recurso. É possível ver essas descobertas em sua conta de administrador delegado do Security Hub usando a agregação entre regiões.

Como uma melhor prática, use as credenciais raiz somente quando necessário para realizar tarefas de gerenciamento de serviços e da conta. Aplique as políticas do diretamente a grupos e funções, mas não aos usuários. Para obter instruções sobre como configurar usuários e grupos do IAM, consulte Criação do seu primeiro usuário do IAM e grupo de administradores no Guia do usuário do IAM.

Correção

As etapas para corrigir esse problema incluem a configuração de um tópico do Amazon SNS, CloudTrail uma trilha, um filtro métrico e um alarme para o filtro métrico.

Para criar um tópico do Amazon SNS

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Crie um tópico do que receba todos os alarmes de CIS.

   Crie pelo menos um assinante para o tópico. Para obter mais informações, consulte Conceitos básicos do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

Em seguida, configure um ativo CloudTrail que se aplique a todas as regiões. Para fazer isso, siga as etapas de correção em the section called "[CloudTrail.1] CloudTrail deve ser habilitado e configurado com pelo menos uma trilha multirregional que inclua eventos de gerenciamento de leitura e gravação".

Anote o nome do grupo de CloudWatch registros de registros que você associa à CloudTrail trilha. Crie filtros métricos para o grupo de logs.

Por fim, crie o filtro métrico e o alarme.

Para criar um filtro e um alarme de métrica

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Grupos de logs.
3. Marque a caixa de seleção do grupo de CloudWatch registros de registros associado à CloudTrail trilha que você criou.
4. Escolha Ações, Criar filtro de métrica.
5. Em Define pattern (Definir padrão), faça o seguinte:
   a. Copie o seguinte padrão e cole-o no campo Filter Pattern (Padrão de filtro).

      ```
      {$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS &&
       $.eventType !="AwsServiceEvent"}
      ```

   b. Escolha Próximo.
6. Em Atribuir métrica, faça o seguinte:
   a. Em Filter name (Nome do filtro), insira um nome para o filtro de métricas de solicitação.
   b. Em Metric Namespace (Namespace da métrica), digite **`LogMetrics`**.

      Se você usar o mesmo namespace para todos os seus filtros de métricas de log do CIS, todas as métricas do CIS Benchmark serão agrupadas.
   c. Em Metric name (Nome da métrica), insira um nome para a nova métrica. O nome da métrica. Você precisará selecionar a métrica ao criar o alarme.
   d. Em Metric Value (Valor de métrica), insira **1**.
   e. Escolha Próximo.
7. Em Revisar e criar, verifique as informações que você forneceu para o novo filtro de métrica. Escolha Create Metric Filter (Criar filtro de métrica).

8. No painel de navegação, escolha Grupos de log e, em seguida, escolha o filtro que você criou em Filtros métricos.
9. Marque a caixa de seleção da UO. Selecione Criar alarme.
10. Em Especificar métrica e condições, insira o seguinte.
    a. Na seção Conditions (Condições), em Threshold type (Tipo de limite), escolha Static (Estático).
    b. Para Definir a condição de alarme, escolha Maior/igual.
    c. Para o valor do limite, insira .
    d. Escolha Próximo.
11. Em Ações do evento, faça o seguinte:
    a. Em Alarm state trigger (Gatilho do estado do alarme), escolha In alarm (Em alarme).
    b. Em Select an SNS topic (Selecionar um tópico do SNS), escolha Select an existing SNS topic (Selecionar um tópico do SNS existente).
    c. Em Actions (Ações), em Send notification to (Enviar notificação para), escolha Enter list (Inserir lista) e insira o nome do tópico que você criou no procedimento anterior.
    d. Escolha Próximo.
12. Em Add a description (Adicionar uma descrição), insira um nome e uma descrição para o alarme e selecione Next (Próximo). Em seguida, escolha Próximo.
13. Em Visualizar e criar, revise a configuração do alarme. Escolha Criar alarme.

As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `iam-policy-no-statements-with-full-access`

Tipo de programação: acionado por alterações

Parâmetros:

- `excludePermissionBoundaryPolicy`: `True` (não personalizável)

Esse controle verifica se as políticas baseadas em identidade do IAM que você cria têm instruções Allow que usam o caractere curinga * para conceder permissões para todas as ações em qualquer serviço. O controle falhará se alguma declaração de política incluir `"Effect": "Allow"` com `"Action": "Service:*"`.

Por exemplo, a declaração a seguir em uma política resulta em uma descoberta malsucedida.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:*",
  "Resource": "*"
}
```

O controle também falhará se você usar `"Effect": "Allow"` com `"NotAction": "service:*"`. Nesse caso, o `NotAction` elemento fornece acesso a todas as ações em um AWS service (Serviço da AWS), exceto às ações especificadas em`NotAction`.

Esse controle se aplica somente às políticas do IAM gerenciadas pelo cliente. Ela não se aplica às políticas do IAM que são gerenciadas pela AWS.

Ao atribuir permissões a Serviços da AWS, é importante definir o escopo das ações permitidas do IAM em suas políticas do IAM. Você deve restringir as ações do IAM somente às ações necessárias. Isso ajuda você a provisionar permissões com privilégios mínimos. Políticas excessivamente permissivas podem levar ao aumento de privilégios se as políticas estiverem vinculadas a uma entidade principal do IAM que talvez não exija a permissão.

Em alguns casos, é possível que você deseje permitir ações do IAM com um prefixo semelhante, como `DescribeFlowLogs` e `DescribeAvailabilityZones`. Nesses casos autorizados, é possível adicionar um curinga com sufixo ao prefixo comum. Por exemplo, `ec2:Describe*`.

Esse controle passa se você usar uma ação prefixada do IAM com um caractere curinga com sufixo. Por exemplo, a declaração a seguir em uma política resulta em uma descoberta malsucedida.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:Describe*",
  "Resource": "*"
}
```

Ao agrupar ações relacionadas do IAM dessa forma, você também pode evitar exceder os limites de tamanho da política do IAM.

> **Note**
>
> AWS Config deve estar habilitado em todas as regiões nas quais você usa o Security Hub. Entretanto, a gravação global de recursos pode ser ativada em uma única região. Se você registrar apenas recursos globais em uma única região, poderá desabilitar esse controle em todas as regiões, exceto na região em que registra recursos globais.

Correção

Para corrigir esse problema, atualize suas políticas do IAM para que elas não permitam privilégios administrativos “*” completos. Para obter mais informações sobre como editar uma política do IAM, consulte Edição de políticas do IAM no Guia do usuário do IAM.

As credenciais de usuário do IAM não utilizadas devem ser removidas

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/1.12, CIS Foundations Benchmark v1.4.0/1.12 AWS

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

AWS Config regra: **`iam-user-unused-credentials-check`**

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se seus usuários do IAM têm senhas ou chaves de acesso ativas que não foram usadas por 90 dias. Para isso, ele verifica se o `maxCredentialUsageAge` parâmetro da AWS Config regra é igual a 45 ou mais.

Os usuários podem acessar AWS recursos usando diferentes tipos de credenciais, como senhas ou chaves de acesso.

Recomendamos que você remova ou desative todas as credenciais que não foram usadas em 90 dias ou mais. Desabilitar ou remover credenciais desnecessárias reduz a possibilidade de uso de credenciais associadas a uma conta comprometida ou abandonada.

A AWS Config regra para esse controle usa as operações de `GenerateCredentialReport`API `GetCredentialReport`e, que são atualizadas somente a cada quatro horas. As alterações feitas nos usuários do podem levar até quatro horas para ficarem visíveis para esse controle.

> **Note**
>
> AWS Config deve estar habilitado em todas as regiões nas quais você usa o Security Hub. Entretanto, a gravação global de recursos pode ser ativada em uma única região. Se você registrar apenas recursos globais em uma única região, poderá desabilitar esse controle em todas as regiões, exceto na região em que registra recursos globais.

Correção

Quando você visualiza as informações do usuário no console do IAM, há colunas para Idade da chave de acesso, Idade da senha e Última atividade. Se o valor em qualquer uma dessas colunas for maior do que 90 dias, deixe as credenciais para esses usuários inativas.

Você também pode usar os relatórios de credenciais para monitorar e identificar as contas de usuário sem atividade por 90 dias ou mais. É possível baixar os relatórios de credenciais no formato .csv no console do IAM `.csv`.

Depois de identificar as contas inativas ou as credenciais não utilizadas, desative-as. Para instruções, consulte Criar, alterar ou excluir uma senha de usuário do IAM (console) no Guia do usuário do IAM.

[IAM.23] Os analisadores do IAM Access Analyzer devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

AWS Config regra: `tagged-accessanalyzer-analyzer` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um analisador gerenciado pelo AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o analisador não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o analisador não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM.

Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um analisador, consulte TagResourcea Referência da API do AWS IAM Access Analyzer.

[IAM.24] As funções do IAM devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

AWS Config regra: `tagged-iam-role` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter.	StringList	Lista de tags que atendem	`No default value`

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	Chaves de tag fazem distinção entre maiúsculas e minúsculas.		aos AWS requisitos	

Esse controle verifica se uma função AWS Identity and Access Management (IAM) tem tags com as chaves específicas definidas no parâmetro `requiredTagKeys`. O controle falhará se a função não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro `requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a função não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com `aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma função do IAM, consulte Como marcar recursos do IAM no Guia do usuário do IAM.

[IAM.25] Os usuários do IAM devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

AWS Config regra: `tagged-iam-user` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um usuário AWS Identity and Access Management (IAM) tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o usuário não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o usuário não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um usuário do IAM, consulte Como marcar recursos do IAM no Guia do usuário do IAM.

[IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/1.19

Categoria: Identificação > Conformidade

Severidade: média

Tipo de recurso

AWS Config regra: **`iam-server-certificate-expiration-check`**

Tipo de programação: Periódico

Parâmetros: nenhum

Isso controla se um certificado de servidor SSL/TLS ativo gerenciado no IAM expirou. O controle falhará se o certificado de servidor SSL/TLS expirado não for removido.

Para habilitar conexões HTTPS com seu site ou aplicativo no AWS, você precisa de um certificado de servidor SSL/TLS. Você pode usar o IAM ou AWS Certificate Manager (ACM) para armazenar e implantar certificados de servidor. Use o IAM como gerenciador de certificados somente quando precisar oferecer suporte a conexões HTTPS em uma conexão Região da AWS que não seja compatível com o ACM. O IAM criptografa com segurança suas chaves privadas e armazena a versão criptografada no armazenamento de certificado SSL do IAM. O IAM oferece suporte à implantação de certificados de servidor em todas as regiões, mas você precisa obter seu certificado de um provedor externo para usá-lo com AWS. Você não pode fazer upload de um certificado do ACM para o IAM. Além disso, você não pode gerenciar seus certificados no console do IAM. A remoção de certificados SSL/TLS expirados elimina o risco de que um certificado inválido seja implantado acidentalmente em um recurso, o que pode prejudicar a credibilidade do aplicativo ou site subjacente.

Correção

Para remover um certificado de servidor do IAM, consulte Gerenciamento de certificados de servidor no IAM no Guia do usuário do IAM.

[IAM.27] As identidades do IAM não devem ter a política anexada AWSCloudShellFullAccess

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/1.22

Categoria: Proteger > Gerenciamento de acesso seguro > Políticas seguras de IAM

Severidade: média

Tipo de recurso:`AWS::IAM::Role`,`AWS::IAM::User`, `AWS::IAM::Group`

AWS Config regra: **`iam-policy-blacklisted-check`**

Tipo de programação: acionado por alterações

Parâmetros:

- “PolicyArns”: “arn:aws:iam: :aws:policy/, arn:aws-cn:iam: :aws:policy/, arn ::iam: AWSCloudShellFullAccess :aws:policy/” AWSCloudShellFullAccess aws-us-gov AWSCloudShellFullAccess

Esse controle verifica se uma identidade do IAM (usuário, função ou grupo) tem a política AWS `AWSCloudShellFullAccess` gerenciada anexada. O controle falhará se uma identidade do IAM tiver a `AWSCloudShellFullAccess` política anexada.

AWS CloudShell fornece uma maneira conveniente de executar comandos CLI contra. Serviços da AWS A política AWS gerenciada `AWSCloudShellFullAccess` fornece acesso total a CloudShell, o que permite a capacidade de upload e download de arquivos entre o sistema local do usuário e o CloudShell ambiente. Dentro do CloudShell ambiente, um usuário tem permissões de sudo e pode acessar a Internet. Como resultado, anexar essa política gerenciada a uma identidade do IAM permite que eles instalem software de transferência de arquivos e movam dados de servidores externos da CloudShell Internet. Recomendamos seguir o princípio do privilégio mínimo e anexar permissões mais restritas às suas identidades do IAM.

Correção

Para separar a `AWSCloudShellFullAccess` política de uma identidade do IAM, consulte Adicionar e remover permissões de identidade do IAM no Guia do usuário do IAM.

[IAM.28] O analisador de acesso externo do IAM Access Analyzer deve estar ativado

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/1.20

Categoria: Detectar > Serviços de detecção > Monitoramento de uso privilegiado

Severidade: alta

Tipo de recurso

AWS Config regra: **`iam-external-access-analyzer-enabled`**

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um Conta da AWS tem um analisador de acesso externo do IAM Access Analyzer ativado. O controle falhará se a conta não tiver um analisador de acesso externo ativado na sua conta atualmente selecionada Região da AWS.

Os analisadores de acesso externo do IAM Access Analyzer ajudam a identificar recursos em sua organização e contas, como buckets do Amazon Simple Storage Service (Amazon S3) ou funções do IAM, que são compartilhados com uma entidade externa. Isso ajuda você a evitar o

acesso não intencional aos seus recursos e dados. O IAM Access Analyzer é regional e deve ser ativado em cada região. Para identificar recursos que são compartilhados com entidades externas, um analisador de acesso usa raciocínio baseado em lógica para analisar as políticas baseadas em recursos em seu ambiente. AWS Ao habilitar um analisador de acesso externo, você cria um analisador para toda a sua organização ou conta.

Correção

Para habilitar um analisador de acesso externo em uma região específica, consulte Habilitar o IAM Access Analyzer no Guia do usuário do IAM. Você deve habilitar um analisador em cada região na qual deseja monitorar o acesso aos seus recursos.

AWS IoT controles

Esses controles estão relacionados aos AWS IoT recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[IoT.1] perfis de AWS IoT Core segurança devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-iot-securityprofile` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o	StringList	Lista de tags que atendem	`No default value`

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.		aos AWS requisitos	

Esse controle verifica se um perfil de AWS IoT Core segurança tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o perfil de segurança não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o perfil de segurança não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um perfil AWS IoT Core de segurança, consulte Como marcar seus AWS IoT recursos no Guia do AWS IoT desenvolvedor.

[IoT.2] as ações de AWS IoT Core mitigação devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-iot-mitigationaction` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se uma AWS IoT Core ação de mitigação tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se a ação de mitigação não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro. `requiredTagKeys` Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a ação de mitigação não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma ação de AWS IoT Core mitigação, consulte Como marcar seus AWS IoT recursos no Guia do AWS IoT desenvolvedor.

[IoT.3] as AWS IoT Core dimensões devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-iot-dimension` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se uma AWS IoT Core dimensão tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a dimensão não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a dimensão não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS

Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma AWS IoT Core dimensão, consulte Como marcar seus AWS IoT recursos no Guia do AWS IoT desenvolvedor.

[IoT.4] os AWS IoT Core autorizadores devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-iot-authorizer` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um AWS IoT Core autorizador tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o autorizador não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave

de tag e falhará se o autorizador não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um AWS IoT Core autorizador, consulte Como marcar seus AWS IoT recursos no Guia do AWS IoT desenvolvedor.

[IoT.5] aliases de AWS IoT Core função devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-iot-rolealias` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um alias de AWS IoT Core função tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o alias da função não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o alias da função não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS

Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um alias de AWS IoT Core função, consulte Como marcar seus AWS IoT recursos no Guia do AWS IoT desenvolvedor.

As AWS IoT Core políticas [IoT.6] devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-iot-policy` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se uma AWS IoT Core política tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a política não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag

e falhará se a política não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma AWS IoT Core política, consulte Como marcar seus AWS IoT recursos no Guia do AWS IoT desenvolvedor.

Controles do Amazon Kinesis

Esses controles estão relacionados aos recursos da API de Gateway.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

Os fluxos do Kinesis devem ser criptografados em repouso

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra do AWS Config : `kinesis-stream-encrypted`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o Kinesis Data Streams está criptografado em repouso com criptografia do lado do servidor. Esse controle verifica se o Kinesis Data Streams está criptografado em repouso com criptografia do lado do servidor.

A criptografia no lado do servidor é um recurso do Amazon Kinesis Data Streams que criptografa automaticamente os dados antes do repouso usando uma chave mestra de cliente (CMK) do AWS KMS key especificada por você. Os dados são criptografados antes de serem gravados na camada de armazenamento do fluxo do Kinesis e descriptografados depois de recuperados do armazenamento. Como resultado, os dados são criptografados em repouso no serviço Amazon Kinesis Data Streams.

Correção

Para obter informações sobre como habilitar a criptografia no lado do servidor para o Kinesis Data Streams, consulte Using Server-Side Encryption no Amazon Kinesis Data Streams Developer Guide.

[Kinesis.2] Os streams do Kinesis devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config: `tagged-kinesis-stream` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um stream de dados do Amazon Kinesis tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o fluxo de dados não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle verificará apenas a existência de uma chave de tag e falhará se o fluxo de dados não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS

Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um stream de dados do Kinesis, consulte Como marcar seus streams no Amazon Kinesis Data Streams no Guia do desenvolvedor do Amazon Kinesis.

AWS Key Management Service controles

Esses controles estão relacionados aos AWS KMS recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `iam-customer-policy-blocked-kms-actions`

Tipo de programação: acionado por alterações

Parâmetros:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt` (não personalizável)
- `excludePermissionBoundaryPolicy`: `True` (não personalizável)

Verifica se a versão padrão das políticas gerenciadas pelo cliente do IAM permite que os diretores usem as ações de AWS KMS descriptografia em todos os recursos. O controle falhará se a política

estiver aberta o suficiente para permitir ações `kms:Decrypt` e `kms:ReEncryptFrom` em todas as chaves do KMS.

O controle verifica somente as chaves KMS no elemento Recurso e não leva em conta nenhuma condição no elemento Condição de uma política. Além disso, o controle avalia as políticas gerenciadas pelo cliente vinculadas e não vinculadas. Ele não verifica políticas em linha ou políticas AWS gerenciadas.

Com AWS KMS, você controla quem pode usar suas chaves KMS e obter acesso aos seus dados criptografados. As políticas do IAM definem quais ações uma identidade (usuário, grupo ou função) pode realizar em quais recursos. Seguindo as melhores práticas de segurança, AWS recomenda que você permita o menor privilégio. Portanto, você deve conceder apenas as permissões necessárias para executar uma tarefa. Caso contrário, o usuário poderá usar chaves que não sejam apropriadas para seus dados.

Em vez de conceder permissões para todas as chaves, determine o conjunto mínimo de chaves que os usuários precisam para acessar os dados criptografados. Em seguida, crie políticas que permitam que os usuários usem somente essas chaves. Por exemplo, não conceda permissão `kms:Decrypt` para todas as chaves do KMS. Em vez disso, permita `kms:Decrypt` somente com chaves em uma região específica para sua conta. Ao adotar o princípio do privilégio mínimo, é possível reduzir o risco de divulgação não intencional de seus dados.

Correção

Para modificar uma política gerenciada pelo cliente do IAM, consulte Editar políticas gerenciadas pelo cliente no Guia do usuário do IAM. Ao editar a política, para o campo `Resource`, forneça o nome do recurso da Amazon (ARN) da chave ou chaves específicas nas quais você deseja permitir ações de decodificação.

As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

- `AWS::IAM::Group`
- `AWS::IAM::Role`
- `AWS::IAM::User`

Regra do AWS Config : `iam-inline-policy-blocked-kms-actions`

Tipo de programação: acionado por alterações

Parâmetros:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt` (não personalizável)

Esse controle verifica se as políticas em linha incorporadas às suas identidades do IAM (função, usuário ou grupo) permitem as ações de AWS KMS descriptografia e recriptografia em todas as chaves do KMS. O controle falhará se a política estiver aberta o suficiente para permitir ações `kms:Decrypt` e `kms:ReEncryptFrom` em todas as chaves do KMS.

O controle verifica somente as chaves KMS no elemento Recurso e não leva em conta nenhuma condição no elemento Condição de uma política.

Com AWS KMS, você controla quem pode usar suas chaves KMS e obter acesso aos seus dados criptografados. As políticas do IAM definem quais ações uma identidade (usuário, grupo ou função) pode realizar em quais recursos. Seguindo as melhores práticas de segurança, AWS recomenda que você permita o menor privilégio. Em outras palavras, você deve conceder às identidades somente as permissões necessárias e somente as chaves necessárias para executar uma tarefa. Caso contrário, o usuário poderá usar chaves que não sejam apropriadas para seus dados.

Em vez de conceder permissões para todas as chaves, determine o conjunto mínimo de chaves que os usuários precisam para acessar os dados criptografados. Em seguida, crie políticas que permitam que os usuários usem somente essas chaves. Por exemplo, não conceda permissão `kms:Decrypt` para todas as chaves do KMS. Em vez disso, permita a permissão somente em chaves específicas em uma região específica da sua conta. Ao adotar o princípio do privilégio mínimo, é possível reduzir o risco de divulgação não intencional de seus dados.

Correção

Para modificar uma política em linha do IAM, consulte Editar políticas em linha no Guia do usuário do IAM. Ao editar a política, para o campo `Resource`, forneça o nome do recurso da Amazon (ARN) da chave ou chaves específicas nas quais você deseja permitir ações de decodificação.

[KMS.3] não AWS KMS keys deve ser excluído acidentalmente

Requisitos relacionados: NIST.800-53.r5 SC-28 (3), NIST.800-53.r5 SC-7 (16)

Categoria: Proteger > Proteção de dados > Proteção contra exclusão de dados

Severidade: crítica

Tipo de recurso

Regra AWS Config : `kms-cmk-not-scheduled-for-deletion-2` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se as chaves KMS estão programadas para exclusão. O controle falhará se uma chave KMS estiver programada para exclusão.

As chaves KMS não podem ser recuperadas depois de excluídas. Os dados criptografados sob uma chave KMS também são permanentemente irrecuperáveis se a chave KMS for excluída. Se dados significativos tiverem sido criptografados em uma chave KMS programada para exclusão, considere descriptografar os dados ou recriptografá-los com uma nova chave KMS, a menos que você esteja executando intencionalmente uma eliminação criptográfica.

Quando uma chave KMS é programada para exclusão, um período de espera obrigatório é imposto para permitir tempo de reverter a exclusão, caso tenha sido agendada por engano. O período de espera padrão é de 30 dias, mas pode ser reduzido para até 7 dias quando a chave KMS está programada para exclusão. Durante o período de espera, a exclusão programada pode ser cancelada e a chave KMS não será excluída.

Para obter informações adicionais sobre a exclusão de chaves KMS, consulte Excluir chaves KMS no Guia do desenvolvedor do AWS Key Management Service .

Correção

Para cancelar uma exclusão programada da chave KMS, consulte Para cancelar a exclusão de chaves em Programar e cancelar a exclusão de chaves (console) no Guia do desenvolvedor do AWS Key Management Service .

A rotação de AWS KMS teclas [KMS.4] deve estar ativada

Requisitos relacionados: PCI DSS v3.2.1/3.6.4, CIS Foundations Benchmark v3.0.0/3.6, CIS Foundations Benchmark v1.4.0/3.8, CIS AWS Foundations Benchmark v1.2.0/2.8, NIST.800-53.r5 SC-12, NIST.800-53.r5 AWS SC-12 (2), NIST.800-53.r5 SC-28 (3) AWS

Categoria: Proteger > Proteção de dados > Criptografia de data-at-rest

Severidade: média

Tipo de recurso

Regra do AWS Config : `cmk-backing-key-rotation-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

AWS KMS permite que os clientes girem a chave de apoio, que é o material chave armazenado AWS KMS e está vinculado ao ID da chave KMS. É a chave de backup usada para executar operações de criptografia, por exemplo, criptografia e descriptografia. No momento, a rotação de chaves automatizada retém todas as chaves de backup anteriores para que a descriptografia de dados criptografados seja transparente.

Recomendamos que você habilite a alternância de chaves de CMK. A rotação de chaves de criptografia ajuda a reduzir o impacto em potencial de uma chave comprometida porque os dados criptografados com uma nova chave não podem ser acessados com uma chave anterior que pode ter sido exposta.

Correção

Para ativar a alternância de chaves KMS, consulte Como ativar e desativar a alternância automática de chaves no Guia do desenvolvedor do AWS Key Management Service .

AWS Lambda controles

Esses controles estão relacionados aos recursos da API de Gateway.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[PCI.lambda.1] As funções do devem proibir o acesso público

Requisitos relacionados: PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/1.3.2,PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

Categoria: Proteger > Configuração de rede segura

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `lambda-function-public-access-prohibited`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se a política baseada em recursos da função do proíbe o acesso público fora da sua conta. O controle falhará se o acesso público for permitido. O controle também falhará se uma função do Lambda for invocada do Amazon S3 e a política não incluir uma condição para limitar o acesso público, como `AWS:SourceAccount`. Recomendamos usar outras condições do S3 junto com `AWS:SourceAccount` em sua política de bucket para um acesso mais refinado.

A função do não deve ser publicamente acessível, pois isso pode permitir o acesso não intencional ao código armazenado na função.

Correção

Para corrigir esse problema, você deve atualizar a política baseada em recursos da sua função para remover permissões ou adicionar a condição `AWS:SourceAccount`. Você só pode atualizar a política baseada em recursos a partir da API Lambda ou. AWS CLI

Para começar, revise a política baseada em recursos no console Lambda. Identifique a declaração de política que tem valores de campo `Principal` que tornam a política pública, como `"*"` ou `{ "AWS": "*" }`.

É possível editar uma política em linha no &console;. Para remover as permissões da função, execute o comando `remove-permission` no AWS CLI.

```
$ aws lambda remove-permission --function-name <function-name> --statement-
id <statement-id>
```

Substitua *<function-name>* pelo nome da função do Lambda e *<statement-id>* pela ID da instrução (`Sid`) que você deseja remover.

[Lambda.2] As funções do devem usar os tempos de execução mais recentes

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Desenvolvimento seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `lambda-function-settings-check`

Tipo de programação: acionado por alterações

Parâmetros:

- `runtime`: `dotnet8, dotnet6, java21, java17, java11, java8.al2, nodejs20.x, nodejs18.x, nodejs16.x, python3.12, python3.11, python3.10, python3.9, python3.8, ruby3.3, ruby3.2` (não personalizável)

Esse controle verifica se as configurações de tempo de execução da AWS Lambda função correspondem aos valores esperados definidos para os tempos de execução suportados em cada idioma. O controle falhará se a função Lambda não usar um tempo de execução compatível, mencionado anteriormente em parâmetros. O Security Hub ignora funções que têm um tipo de pacote `deImage`.

Os tempos de execução do se baseiam em uma combinação de sistema operacional, linguagem de programação e bibliotecas de software que estão sujeitos a manutenção e atualizações de segurança. Quando um componente de tempo de runtime não é mais compatível com as atualizações de segurança, o runtime defasa o componente. Mesmo que você não possa criar funções que usem o tempo de execução obsoleto, a função ainda está disponível para processar eventos de invocação. Recomendamos garantir que suas funções do Lambda estejam atualizadas e não usem ambientes de tempo de execução obsoletos. Para obter uma lista dos tempos de

execução compatíveis, consulte os tempos de execução do Lambda no AWS Lambda Guia do desenvolvedor.

Correção

Para obter mais informações sobre runtimes compatíveis e programações de suspensão de uso, consulte Política de suspensão de runtime no Guia do desenvolvedor do AWS Lambda . Ao migrar os tempos de execução para a versão mais recente, siga a sintaxe e as orientações dos editores de idioma. Também recomendamos aplicar atualizações de tempo de execução para ajudar a reduzir o risco de impacto em suas cargas de trabalho no caso raro de uma incompatibilidade de versão em tempo de execução.

[PCI.Lambda.2] As funções do Lambda devem estar em uma VPC

Requisitos relacionados: PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/1.3.2,PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

Categoria: Proteger > Configuração de rede segura

Severidade: baixa

Tipo de recurso

AWS Config regra: **`lambda-inside-vpc`**

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma função Lambda está implantada em uma nuvem privada virtual (VPC). O controle falhará se a função Lambda não for implantada em uma VPC. O Security Hub não avalia a configuração de roteamento de sub-rede da VPC para determinar a acessibilidade pública. É possível ver falhas nas descobertas dos recursos do Lambda @Edge.

A implantação de recursos em uma VPC fortalece a segurança e o controle sobre as configurações de rede. Essas implantações também oferecem escalabilidade e alta tolerância a falhas em várias zonas de disponibilidade. Você pode personalizar as implantações de VPC para atender aos diversos requisitos de aplicativos.

Correção

Para configurar uma função existente para se conectar a sub-redes privadas em sua VPC, consulte Configurar o acesso à VPC no Guia do desenvolvedor do AWS Lambda . Recomendamos escolher pelo menos duas sub-redes privadas para alta disponibilidade e pelo menos um grupo de segurança que atenda aos requisitos de conectividade da função.

[Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra do AWS Config : `lambda-vpc-multi-az-check`

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`availabilityZones`	Número mínimo de zonas de disponibilidade	Enum	`2, 3, 4, 5, 6`	2

Esse controle verifica se uma AWS Lambda função que se conecta a uma nuvem privada virtual (VPC) opera em pelo menos o número especificado de zonas de disponibilidade (AZs). O controle falhará se a função não operar em pelo menos o número especificado de AZs. A menos que você forneça um valor de parâmetro personalizado para o número mínimo de AZs, o Security Hub usará um valor padrão de duas AZs.

A implantação de recursos em várias AZs é uma prática AWS recomendada para garantir a alta disponibilidade em sua arquitetura. A disponibilidade é um pilar fundamental no modelo de segurança da tríade confidencialidade, integridade e disponibilidade. Todas as funções do Lambda que se conectem a uma VPC devem ter uma implantação Multi-AZ para garantir que uma única zona de falha não cause uma interrupção total das operações.

Correção

Se você configurar a função para se conectar a uma nuvem privada virtual (VPC) na sua conta, especifique sub-redes em várias zonas de disponibilidade para garantir uma alta disponibilidade. Para obter instruções, consulte Configurar acesso à VPC no Guia do desenvolvedor do AWS Lambda .

Alta disponibilidade: o Lambda executa sua função em várias zonas de disponibilidade para garantir que ela esteja disponível para processar eventos no caso de uma interrupção do serviço em uma única zona.

[Lambda.6] As funções Lambda devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-lambda-function` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	entre maiúsculas e minúsculas.			

Esse controle verifica se uma AWS Lambda função tem tags com as teclas específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a função não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a função não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma função Lambda, consulte Como usar tags em funções do Lambda no Guia do desenvolvedor.AWS Lambda

Controles do Amazon Macie

Esses controles estão relacionados a recursos do Macie.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[Macie.1] O Amazon Macie deve estar ativado

Requisitos relacionados: NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9(1), NIST.800-53.r5 RA-5, NIST.800-53.r5 SA-8(19), NIST.800-53.r5 SI-4

Categoria: Detectar > Serviços de detecção

Severidade: média

Tipo de recurso

Regra do AWS Config : `macie-status-check`

Tipo de programação: Periódico

Esse controle verifica se o Amazon Macie está habilitado para uma conta. O controle falhará se o Macie não estiver habilitado para a conta.

O Amazon Macie descobre dados sigilosos usando machine learning e correspondência de padrões, fornece visibilidade dos riscos de segurança de dados e permite proteção automatizada contra esses riscos. O Macie avalia automática e continuamente seus buckets do Amazon Simple Storage Service (Amazon S3) quanto à segurança e ao controle de acesso, e gera descobertas para notificá-lo sobre possíveis problemas com a segurança ou a privacidade de seus dados do Amazon S3. O Macie também automatiza a descoberta e a reportagem de dados sigilosos, como as informações de identificação pessoal (PII), para você compreender melhor os dados armazenados por você no Amazon S3. Para saber mais, consulte o Guia do usuário do Amazon Macie.

Correção

Para habilitar o Macie, consulte Habilitar o Macie no Guia do usuário do Amazon Macie.

[Macie.2] A descoberta automatizada de dados confidenciais do Macie deve ser ativada

Requisitos relacionados: NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9(1), NIST.800-53.r5 RA-5, NIST.800-53.r5 SA-8(19), NIST.800-53.r5 SI-4

Categoria: Detectar > Serviços de detecção

Severidade: alta

Tipo de recurso

Regra do AWS Config : `macie-auto-sensitive-data-discovery-check`

Tipo de programação: Periódico

Esse controle verifica se a descoberta automatizada de dados confidenciais está habilitada para uma conta de administrador do Amazon Macie. O controle falhará se a descoberta automatizada de dados confidenciais não estiver habilitada para uma conta de administrador do Macie. Esse controle se aplica somente às contas de administrador.

O Macie automatiza a descoberta e a emissão de relatórios de dados confidenciais, como informações de identificação pessoal (PII), em buckets do Amazon Simple Storage Service (Amazon S3). Com a descoberta automatizada de dados confidenciais, o Macie avalia continuamente seu inventário de buckets e usa técnicas de amostragem para identificar e selecionar objetos S3 representativos de seus buckets. Em seguida, Macie analisa os objetos selecionados, inspecionando-os em busca de dados confidenciais. Conforme as análises progridem, o Macie atualiza estatísticas, dados de inventário e outras informações que ele fornece sobre seus dados do S3. O Macie também gera descobertas para relatar os dados confidenciais que encontra.

Correção

Para criar e configurar trabalhos automatizados de descoberta de dados confidenciais para analisar objetos em buckets do S3, consulte Como configurar a descoberta automática de dados confidenciais para sua conta no Guia do usuário do Amazon Macie.

Controles do Amazon EKS

Amazon Managed Streaming for Apache Kafka: para solucionar problemas relacionados ao Amazon MSK Connect.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

Os clusters MSK devem ser criptografados em trânsito entre os nós do agente

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso

Regra do AWS Config : `msk-in-cluster-node-require-tls`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster Amazon MSK está criptografado em trânsito com HTTPS (TLS) entre os nós intermediários do cluster. O controle falhará se a comunicação de texto simples estiver habilitada para uma conexão de nó do agente do cluster.

O HTTPS oferece uma camada extra de segurança, pois usa TLS para mover dados e pode ser usado para ajudar a impedir que possíveis invasores usem ataques semelhantes para espionar person-in-the-middle ou manipular o tráfego da rede. Por padrão, o Amazon MSK criptografa dados em trânsito com TLS. É possível substituir esse padrão no momento de criação do cluster. Recomendamos o uso de conexões criptografadas via HTTPS (TLS) para conexões de nós do agente.

Correção

Para atualizar as configurações de criptografia para clusters MSK, consulte Atualizar configurações de segurança de um cluster no Guia do desenvolvedor do Amazon Managed Streaming for Apache Kafka.

[MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado

Requisitos relacionados: NIST.800-53.r5 SI-4 (12), NIST.800-53.r5 SI-4 (5)

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `msk-enhanced-monitoring-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster Amazon MSK tem um monitoramento aprimorado configurado, especificado por um nível de monitoramento de pelo menos `PER_TOPIC_PER_BROKER`. O controle falhará se o nível de monitoramento do cluster estiver definido como `DEFAULT` ou `PER_BROKER`.

O nível de monitoramento `PER_TOPIC_PER_BROKER` fornece insights mais granulares sobre a performance do seu cluster do MSK e também fornece métricas relacionadas à utilização de recursos, como uso de CPU e memória. Isso ajuda você a identificar gargalos de performance e padrões de utilização de recursos para tópicos e agentes individuais. Essa visibilidade, por sua vez, pode otimizar a performance dos seus agentes do Kafka.

Correção

Para configurar o monitoramento aprimorado para um cluster do MSK, conclua as etapas a seguir:

1. Abra o console do Amazon MSK em https://console.aws.amazon.com/msk/home?region=us-east-1#/home/.
2. No painel de navegação, escolha Clusters. Em seguida, escolha um cluster.
3. Em Ação, selecione Editar monitoramento.
4. Selecione a opção para Monitoramento aprimorado em nível de tópico.
5. Escolha Salvar alterações.

Para obter mais informações sobre os níveis de monitoramento, consulte Atualização das configurações de segurança de um cluster no Guia do desenvolvedor do Amazon Managed Streaming for Apache Kafka.

Controles do Amazon MQ

Esses controles estão relacionados aos recursos da API de Gateway.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch

Requisitos relacionados: NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-12, Nist.800-53.r5 SI-4

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `mq-cloudwatch-audit-log-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um agente do Amazon MQ ActiveMQ transmite logs de auditoria para o Amazon Logs. CloudWatch O controle falhará se o agente não transmitir os registros de auditoria para o CloudWatch Logs.

Ao publicar os registros do agente ActiveMQ no Logs CloudWatch , você pode CloudWatch criar alarmes e métricas que aumentam a visibilidade das informações relacionadas à segurança.

Correção

Para transmitir os logs do agente ActiveMQ para o Logs, consulte Configurando o Amazon MQ CloudWatch para registros do ActiveMQ no Guia do Desenvolvedor do Amazon MQ.

[MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada

Requisitos relacionados: NIST.800-53.r5 CM-3, NIST.800-53.r5 SI-2

Categoria: Detectar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `mq-auto-minor-version-upgrade-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um agente do Amazon MQ tem a atualização automática de versões secundárias ativada. O controle falhará se o corretor não tiver a atualização automática de versões secundárias ativada.

À medida que o Amazon MQ lança e oferece suporte a novas versões do broker engine, as alterações são compatíveis com versões anteriores de um aplicativo existente e não substituem a funcionalidade existente. As atualizações automáticas da versão do broker engine protegem você contra riscos de segurança, ajudam a corrigir bugs e aprimoram a funcionalidade.

> **Note**
>
> Quando o broker associado à atualização automática de versões secundárias está em seu patch mais recente e não tem suporte, você deve realizar uma ação manual para fazer o upgrade.

Correção

Para habilitar a atualização automática de versões secundárias para um agente de MQ, consulte Atualização automática da versão secundária do mecanismo no Guia do desenvolvedor do Amazon MQ.

[MQ.4] Os corretores do Amazon MQ devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-amazonmq-broker` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um agente do Amazon MQ tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o corretor não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o broker não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS

Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um agente do Amazon MQ, consulte Recursos de marcação no Guia do desenvolvedor do Amazon MQ.

Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `mq-active-deployment-mode`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o modo de implantação de um agente Amazon MQ ActiveMQ está definido como ativo/em espera. O controle falhará se um agente de instância única (ativado por padrão) for definido como o modo de implantação.

A implantação ativa/em espera fornece alta disponibilidade para seus agentes do Amazon MQ ActiveMQ em uma Região da AWS. O modo de implantação ativo/em espera inclui duas instâncias de agente em duas zonas de disponibilidade diferentes, configuradas em um par redundante. Esses agentes se comunicam de forma síncrona com seu aplicativo, o que pode reduzir o tempo de inatividade e a perda de dados em caso de falha.

Correção

Para criar um novo agente ActiveMQ com modo de implantação ativo/em espera, consulte Criar e configurar um agente ActiveMQ no Guia do desenvolvedor do Amazon MQ. Em Modo de implantação, escolha Operador ativo/em espera de alta disponibilidade. Não é possível alterar o

modo de implantação de um agente existente. Em vez disso, você deve criar um novo agente e copiar as configurações do agente antigo.

Os agentes do RabbitMQ devem usar o modo de implantação de cluster

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `mq-rabbit-deployment-mode`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o modo de implantação de um agente Amazon MQ ActiveMQ está definido como ativo/em espera. O controle falhará se um agente de instância única (ativado por padrão) for definido como o modo de implantação.

A implantação ativa/em espera fornece alta disponibilidade para seus agentes do Amazon MQ ActiveMQ em uma Região da AWS. A implantação do cluster é um agrupamento lógico de três nós de agente do RabbitMQ, cada um com seu próprio volume do Amazon Elastic Block Store (Amazon EBS) e um estado compartilhado. A implantação do cluster garante que os dados sejam replicados para todos os nós do cluster, o que pode reduzir o tempo de inatividade e a perda de dados em caso de falha.

Correção

Para criar um novo agente ActiveMQ com modo de implantação ativo/em espera, consulte Criar e configurar um agente ActiveMQ no Guia do desenvolvedor do Amazon MQ. Para Deployment mode, escolha Single-broker deployment. Não é possível alterar o modo de implantação de um agente existente. Em vez disso, você deve criar um novo agente e copiar as configurações do agente antigo.

Controles do Amazon Neptune

Esses controles estão relacionados aos recursos da API de Gateway.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

Os clusters de banco de dados Neptune devem ser criptografados em repouso

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra do AWS Config : `neptune-cluster-encrypted`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster do Amazon DocumentDB é criptografado em repouso. O controle falhará se um cluster de banco de dados Neptune não estiver criptografado em repouso.

Dados em repouso se referem a qualquer dado armazenado em armazenamento persistente e não volátil por qualquer período. A criptografia ajuda a proteger a confidencialidade desses dados, reduzindo o risco de que um usuário não autorizado possa acessá-los. Criptografar seus clusters de banco de dados Neptune protege seus dados e metadados contra acesso não autorizado. Ele também atende aos requisitos de conformidade para data-at-rest criptografia de sistemas de arquivos de produção.

Correção

É possível ativar a criptografia em repouso ao criar um cluster do Neptune DB. Não é possível alterar as configurações de criptografia após a criação de um cluster. Para obter mais informações, consulte Criptografar recursos do Neptune em repouso no Guia do usuário do Neptune.

[Neptune.2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(1), NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-6(5),

NIST.800-53.r5 AU-7(1), NIST.800-53.r5 AU-9(7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-4(5), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `neptune-cluster-cloudwatch-log-export-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster de banco de dados Neptune publica registros de auditoria no Amazon Logs. CloudWatch O controle falhará se um cluster de banco de dados Neptune não publicar registros de auditoria no Logs. CloudWatch `EnableCloudWatchLogsExport`deve ser definido como`Audit`.

O Amazon Neptune e o CloudWatch Amazon são integrados para que você possa coletar e analisar métricas de desempenho. O Neptune envia métricas automaticamente e também oferece suporte CloudWatch a alarmes. CloudWatch Os registros em log de auditoria são altamente personalizáveis. Quando você audita um banco de dados, cada operação nos dados pode ser monitorada e registrada em log em uma trilha de auditoria, incluindo informações sobre qual cluster de banco de dados é acessado e como. Recomendamos enviar esses registros para ajudá-lo CloudWatch a monitorar seus clusters de banco de dados Neptune.

Correção

Para publicar registros de auditoria do Neptune no Logs, consulte CloudWatch Publicar registros do Neptune no CloudWatch Amazon Logs no Guia do usuário do Neptune. Na seção Exportações de logs, escolha Auditoria.

Os instantâneos do cluster de banco de dados Neptune não devem ser públicos

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Configuração de rede segura > Recursos não acessíveis ao público

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `neptune-cluster-snapshot-public-prohibited`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um instantâneo de cluster manual do Amazon DocumentDB é público. O controle falhará se o instantâneo manual do cluster for público.

Um instantâneo manual do cluster de banco de dados Neptune não deve ser público, a menos que pretendido. Se você compartilhar um instantâneo manual não criptografado como público, isso o disponibilizará para todas as contas da AWS. Instantâneos públicos podem resultar em exposição não intencional de dados.

Correção

Para remover o acesso público aos instantâneos manuais do cluster de banco de dados do Neptune, consulte Compartilhar um instantâneo do cluster do banco de dados no Guia do usuário do Neptune.

[Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Proteger > Proteção de dados > Proteção contra exclusão de dados

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `neptune-cluster-deletion-protection-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster de banco de dados do Neptune tem a proteção contra exclusão habilitada. O controle falhará se o cluster não tiver a proteção contra exclusão habilitada.

A ativação da proteção contra exclusão de clusters oferece uma camada adicional de proteção contra a exclusão acidental do banco de dados ou a exclusão por um usuário não autorizado. O cluster global não pode ser excluído quando a proteção contra exclusão está habilitada. Primeiro, você deve desativar a proteção contra exclusão para que uma solicitação de exclusão possa ser bem-sucedida.

Correção

Para ativar a proteção contra exclusão de um cluster de banco de dados Neptune existente, consulte Modificar o cluster de banco de dados usando o console, a CLI e a API no Guia do usuário do Amazon Aurora.

Os clusters de banco de dados Neptune devem ter backups automatizados habilitados

Requisitos relacionados: NIST.800-53.r5 CA-7

Categoria: Recuperação > Resiliência > Backups ativados

Severidade: média

Tipo de recurso

Regra do AWS Config : `neptune-cluster-backup-retention-check`

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`minimumBackupRetentionPeriod`	Período mínimo de retenção de backups em dias	Inteiro	7 para 35	7

Esse controle verifica se um cluster de banco de dados do Neptune tem backups automáticos habilitados e um período de retenção de backups maior ou igual ao período de tempo especificado.

O controle falhará se os backups não estiverem habilitados para o cluster de banco de dados do Neptune ou se o período de retenção for inferior ao período de tempo especificado. A menos que você forneça um valor de parâmetro personalizado para o período de retenção do backup, o Security Hub usará um valor padrão de 7 dias.

Os backups ajudam você a se recuperar mais rapidamente de um incidente de segurança e a fortalecer a resiliência de seus sistemas. Ao automatizar backups para seus clusters do Neptune DB, será possível restaurar seus sistemas em um determinado momento e minimizar o tempo de inatividade e a perda de dados.

Correção

Para habilitar backups automatizados e definir um período de retenção de backups para seus clusters de banco de dados do Neptune, consulte Habilitação de backups automatizados no Guia do usuário do Amazon RDS. Em Backup, escolha um valor maior ou igual a 7.

Os clusters de banco de dados Neptune devem ser criptografados em repouso

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra do AWS Config : `neptune-cluster-snapshot-encrypted`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um instantâneo do cluster de banco de dados Neptune está criptografado em repouso. O controle falhará se um cluster de banco de dados Neptune não estiver criptografado em repouso.

Dados em repouso se referem a qualquer dado armazenado em armazenamento persistente e não volátil por qualquer período. A criptografia ajuda a proteger a confidencialidade desses dados, reduzindo o risco de que um usuário não autorizado possa acessá-los. Os dados nos clusters do Amazon DocumentDB devem ser criptografados em repouso para uma camada adicional de segurança.

Correção

Você não pode criptografar um instantâneo existente do cluster de banco de dados Neptune. Em vez disso, você deve restaurar o instantâneo em um novo cluster de banco de dados e habilitar a criptografia no cluster. Assim, é possível restaurar um cluster de banco de dados criptografado do instantâneo criptografado. Para obter instruções, consulte Restaurar a partir de um instantâneo de cluster de banco de dados e Criar um instantâneo de cluster de banco de dados no Neptune no Guia do usuário do Neptune.

[Neptune.7] Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada

Requisitos relacionados: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6

Categoria: Proteger > Gerenciamento de acesso seguro > Autenticação sem senha

Severidade: média

Tipo de recurso

Regra do AWS Config : `neptune-cluster-iam-database-authentication`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster de banco de dados Neptune tem a autenticação de banco de dados IAM habilitada. O controle falhará se a autenticação do banco de dados do IAM não estiver habilitada para um cluster de banco de dados Neptune.

A autenticação do banco de dados do IAM para clusters de banco de dados do Amazon Neptune elimina a necessidade de armazenar as credenciais de usuário na configuração do banco de dados, pois a autenticação é gerenciada externamente usando o IAM. Quando a autenticação do banco de dados do IAM está ativada, cada solicitação precisa ser assinada usando o AWS Signature Version 4.

Correção

Por padrão, a autenticação de banco de dados do IAM está desabilitada quando você cria um cluster de banco de dados do &neptune;. Para habilitá-lo, consulte Habilitar a autenticação do banco de dados do IAM no Neptune no Guia do usuário do Neptune.

Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `neptune-cluster-copy-tags-to-snapshot-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster de banco de dados Neptune está configurado para copiar todas as tags para instantâneos quando os instantâneos são criados. O controle falhará se um cluster de banco de dados Neptune não estiver configurado para copiar tags para instantâneos.

A identificação de seus ativos de TI é um aspecto essencial de governança e segurança. Você deve marcar instantâneos da mesma forma que os clusters de banco de dados do Amazon RDS primário. A cópia de tags garante que os metadados dos DB instantâneos correspondam aos da instância de banco de dados de origem e que quaisquer políticas de acesso do DB instantâneo também correspondam às da instância de banco de dados de origem.

Correção

Para copiar tags em instantâneos para clusters de banco de dados Neptune, consulte Copiar tags no Neptune no Guia do usuário do Neptune.

[Neptune.9] Os clusters de banco de dados do Neptune devem ser implantados em várias zonas de disponibilidade

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra do AWS Config : `neptune-cluster-multi-az-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster de banco de dados do Amazon Neptune tem instâncias de réplica de leitura em várias zonas de disponibilidade (AZs). O controle falhará se o cluster for implantado em apenas uma AZ.

Se uma AZ não estiver disponível e durante eventos de manutenção regulares, as réplicas de leitura servirão como destinos de failover para a instância primária. Ou seja, se a instância principal falhar, o Neptune promoverá uma instância de réplica de leitura para se tornar a instância principal. Por outro lado, se o cluster de banco de dados não incluir nenhuma instância de réplica de leitura, o cluster de banco de dados permanecerá indisponível quando a instância primária falhar até que seja recriada. Recriar a instância primária leva muito mais tempo do que promover uma réplica de leitura. Para garantir a alta disponibilidade, recomendamos criar uma ou mais instâncias de réplica de leitura que tenham a mesma classe de instância de banco de dados da instância primária e estejam localizadas em AZs diferentes da instância primária.

Correção

Para implantar um cluster de banco de dados do Neptune em várias AZs, consulte Instâncias de banco de dados de réplica de leitura em um cluster de banco de dados do Neptune no Guia do usuário do Neptune.

AWS Network Firewall controles

Esses controles estão relacionados aos recursos do Firewall de Rede.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[NetworkFirewall.1] Os firewalls do Network Firewall devem ser implantados em várias zonas de disponibilidade

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra do AWS Config : `netfw-multi-az-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle avalia se um firewall gerenciado AWS Network Firewall está implantado em várias zonas de disponibilidade (AZs). O controle falhará se um firewall for implantado em apenas uma AZ.

AWS a infraestrutura global inclui vários Regiões da AWS. As AZs são locais fisicamente separados e isolados dentro de cada região, conectados por redes de baixa latência, alto throughput e altamente redundantes. Ao implantar um firewall do Network Firewall em várias AZs, é possível equilibrar e deslocar o tráfego entre as AZs, o que ajuda a projetar soluções altamente disponíveis.

Correção

Implantação de um firewall do Network Firewall em várias AZs

1. Abra o console do Amazon VPC em https://console.aws.amazon.com/vpc/.
2. No painel de navegação, em Network Firewall, escolha Firewalls.
3. Na página Firewalls, selecione o firewall que você deseja editar.
4. Na página de detalhes do firewall, escolha a guia Detalhes do firewall.
5. Na seção Política associada e VPC, escolha Editar
6. Para adicionar uma nova AZ, escolha Adicionar nova sub-rede. Selecione a AZ e a sub-rede que você gostaria de usar. Certifique-se de selecionar pelo menos duas AZs.
7. Escolha Salvar.

[NetworkFirewall.2] O registro do Firewall de Rede deve estar ativado

Requisitos relacionados: CIS Foundations Benchmark v1.2.0/2.1, CIS Foundations Benchmark v1.4.0/3.1, NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-14(1), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8), NIST.800-53.r5 SA-8(22)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `netfw-logging-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o registro está habilitado para um AWS Network Firewall firewall. O controle falhará se o registro em log não estiver habilitado para pelo menos um tipo de log, ou se o destino dos logs não existir.

O registro em log ajuda a manter a confiabilidade, a disponibilidade e a performance dos seus firewalls. No Network Firewall, os logs apresentam informações detalhadas sobre o tráfego de rede, incluindo a hora em que o mecanismo com estados recebeu um fluxo de pacotes, informações detalhadas sobre o fluxo de pacotes e qualquer ação de regra com estados realizada no fluxo de pacotes.

Correção

Para habilitar o registro em log em um firewall, consulte Atualização da configuração de registro em log de um firewall no Guia do desenvolvedor do AWS Network Firewall .

[NetworkFirewall.3] As políticas de Firewall de Rede devem ter pelo menos um grupo de regras associado

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso

Regra do AWS Config : `netfw-policy-rule-group-associated`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma política de Firewall de rede tem algum grupo de regras com ou sem estado associado. O controle falhará se grupos de regras sem estado ou com estado não forem atribuídos.

Uma política de firewall define como seu firewall monitora e gerencia o tráfego na Amazon Virtual Private Cloud (Amazon VPC). A configuração de grupos de regras sem estado e com estado ajuda a filtrar pacotes e fluxos de tráfego e define o tratamento padrão do tráfego.

Correção

Para adicionar um grupo de regras a uma política de Firewall de rede, consulte Atualizar uma política de firewall no Guia do desenvolvedor do AWS Network Firewall . Para obter informações sobre a criação e o gerenciamento de usuários e grupos, consulte Usuários e grupos do IAM AWS Network Firewall.

[NetworkFirewall.4] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar pacotes completos

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso

Regra do AWS Config : `netfw-policy-default-action-full-packets`

Tipo de programação: acionado por alterações

Parâmetros:

- `statelessDefaultActions: aws:drop,aws:forward_to_sfe` (não personalizável)

Esse controle verifica se a ação sem estado padrão para pacotes completos de uma política de Firewall de rede é descartar ou encaminhar. O controle é aprovado se `Drop` ou `Forward` for selecionado e falha se `Pass` for selecionado.

Uma política de firewall define como seu firewall monitora e gerencia o tráfego na Amazon Virtual Private Cloud (Amazon VPC). Você configura grupos de regras sem estado e com estado para filtrar pacotes e fluxos de tráfego. O padrão `Pass` pode permitir tráfego não intencional.

Correção

Para adicionar um grupo de regras a uma política de Firewall de rede, consulte Atualizar uma política de firewall no Guia do desenvolvedor do AWS Network Firewall . Em Ações padrão sem estado, escolha Editar. Em seguida, escolha Remover ou Encaminhar para grupos de regras com estado como a Ação.

[NetworkFirewall.5] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar para pacotes fragmentados

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso

Regra do AWS Config : `netfw-policy-default-action-fragment-packets`

Tipo de programação: acionado por alterações

Parâmetros:

- `statelessFragDefaultActions (Required) : aws:drop, aws:forward_to_sfe` (não personalizável)

Esse controle verifica se a ação sem estado padrão para pacotes completos de uma política de Firewall de rede é descartar ou encaminhar. O controle é aprovado se `Drop` ou `Forward` for selecionado e falha se `Pass` for selecionado.

Uma política de firewall define como seu firewall monitora e gerencia o tráfego na Amazon Virtual Private Cloud (Amazon VPC). Você configura grupos de regras sem estado e com estado para filtrar pacotes e fluxos de tráfego. O padrão `Pass` pode permitir tráfego não intencional.

Correção

Para adicionar um grupo de regras a uma política de Firewall de rede, consulte Atualizar uma política de firewall no Guia do desenvolvedor do AWS Network Firewall . Em Ações padrão sem estado, escolha Editar. Em seguida, escolha Remover ou Encaminhar para grupos de regras com estado como a Ação.

[NetworkFirewall.6] O grupo de regras do Stateless Network Firewall não deve estar vazio

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso

Regra do AWS Config : `netfw-stateless-rule-group-not-empty`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um grupo de regras sem estado AWS Network Firewall contém regras. O controle falhará se não houver regras no grupo de regras.

Um grupo de regras contém regras que definem como seu firewall processa o tráfego em sua VPC. Um grupo de regras sem estado vazio, quando presente em uma política de firewall, pode dar a impressão de que o grupo de regras processará o tráfego. Entretanto, quando o grupo de regras sem estado está vazio, ele não processa o tráfego.

Correção

Para adicionar regras ao seu grupo de regras do Firewall de rede, consulte Atualizar um grupo de regras com estado no Guia do desenvolvedor do AWS Network Firewall . Na página de detalhes do firewall, em Grupo de regras sem estado, escolha Editar para adicionar regras.

[NetworkFirewall.7] Os firewalls do Firewall de Rede devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-networkfirewall-firewall` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um AWS Network Firewall firewall tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o firewall não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o firewall não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS

Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um firewall do Network Firewall, consulte AWS Network Firewall Recursos de marcação no Guia do AWS Network Firewall desenvolvedor.

[NetworkFirewall.8] As políticas de firewall do Network Firewall devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-networkfirewall-firewallpolicy` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se uma política de AWS Network Firewall firewall tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a política de

firewall não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a política de firewall não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma política de Firewall de Rede, consulte AWS Network Firewall Recursos de marcação no Guia do AWS Network Firewall Desenvolvedor.

[NetworkFirewall.9] Os firewalls do Firewall de Rede devem ter a proteção contra exclusão ativada

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Proteger > Segurança de rede > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra do AWS Config : `netfw-deletion-protection-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um AWS Network Firewall firewall tem a proteção contra exclusão ativada. O controle falhará se a proteção contra exclusão não estiver habilitada para um firewall.

AWS Network Firewall é um firewall de rede gerenciado e com estado e serviço de detecção de intrusões que permite inspecionar e filtrar o tráfego de, para ou entre suas nuvens privadas virtuais (VPCs). A configuração de proteção contra exclusão protege contra a exclusão acidental do firewall.

Correção

Para ativar a proteção contra exclusão em um firewall existente do Firewall de rede, consulte Atualizar um firewall no Guia do desenvolvedor do AWS Network Firewall . Em Alterar proteções, selecione Ativar. Você também pode ativar a proteção contra exclusão invocando a UpdateFirewallDeleteProtectionAPI e definindo o `DeleteProtection` campo como. `true`

Controles OpenSearch do Amazon Service

Esses controles estão relacionados aos recursos OpenSearch do Serviço.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada

Requisitos relacionados: PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/7.2.1, NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra do AWS Config : `opensearch-encrypted-at-rest`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os OpenSearch domínios têm a encryption-at-rest configuração ativada. Ocorrerá uma falha na verificação se a criptografia em repouso não estiver habilitada.

Para uma camada adicional de segurança para dados confidenciais, você deve configurar seu domínio de OpenSearch serviço para ser criptografado em repouso. Quando você configura a criptografia de dados em repouso, AWS KMS armazena e gerencia suas chaves de criptografia. Para realizar a criptografia, AWS KMS usa o algoritmo Advanced Encryption Standard com chaves de 256 bits (AES-256).

Para saber mais sobre a criptografia OpenSearch de serviços em repouso, consulte Criptografia de dados em repouso para o Amazon OpenSearch Service no Amazon OpenSearch Service Developer Guide.

Correção

Para habilitar a criptografia em repouso para OpenSearch domínios novos e existentes, consulte Habilitar a criptografia de dados em repouso no Amazon OpenSearch Service Developer Guide.

Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público

Requisitos relacionados: PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/1.3.2,PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

Categoria: Proteger > Configuração de rede segura

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `opensearch-in-vpc-only`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os OpenSearch domínios estão em uma VPC. Ele não avalia a configuração de roteamento da sub-rede da VPC para determinar a acessibilidade pública.

Você deve garantir que os OpenSearch domínios não estejam vinculados a sub-redes públicas. Consulte as políticas baseadas em recursos no Amazon OpenSearch Service Developer Guide. Você também deve garantir que a VPC esteja configurada de acordo com as melhores práticas recomendadas. Para saber mais, consulte Grupos de segurança para a VPC no Manual do usuário do Amazon VPC.

OpenSearch os domínios implantados em uma VPC podem se comunicar com os recursos da VPC pela AWS rede privada, sem a necessidade de atravessar a Internet pública. Essa configuração aumenta a postura de segurança ao limitar o acesso aos dados em trânsito. As VPCs fornecem vários controles de rede para proteger o acesso aos OpenSearch domínios, incluindo ACL de rede e grupos de segurança. O Security Hub recomenda que você migre OpenSearch domínios públicos para VPCs para aproveitar esses controles.

Correção

Se você criar um domínio com um endpoint público, não será possível colocá-lo em uma VPC posteriormente. Em vez disso, você deve criar um novo domínio e migrar seus dados. O inverso também é verdadeiro. Se você criar um domínio com uma VPC, ele não poderá ter um endpoint público. Em vez disso, você deve criar outro domínio ou desabilitar esse controle.

Para obter instruções, consulte Lançamento de seus domínios do Amazon OpenSearch Service em uma VPC no OpenSearch Amazon Service Developer Guide.

Os OpenSearch domínios [Opensearch.3] devem criptografar os dados enviados entre os nós

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em trânsito

Severidade: média

Tipo de recurso

Regra do AWS Config : `opensearch-node-to-node-encryption-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os OpenSearch domínios têm a node-to-node criptografia ativada. Esse controle falhará se a node-to-node criptografia estiver desativada no domínio.

O HTTPS (TLS) pode ser usado para ajudar a impedir que possíveis invasores espionem ou manipulem o tráfego da rede usando ataques similares. person-in-the-middle Somente conexões criptografadas por HTTPS (TLS) devem ser permitidas. A ativação da node-to-node criptografia para OpenSearch domínios garante que as comunicações dentro do cluster sejam criptografadas em trânsito.

Pode haver uma penalidade de desempenho associada a essa configuração. Você deve estar ciente e testar a compensação de desempenho antes de ativar essa opção.

Correção

Para habilitar a node-to-node criptografia em um OpenSearch domínio, consulte Como ativar a node-to-node criptografia no Amazon OpenSearch Service Developer Guide.

O registro de erros de OpenSearch domínio [Opensearch.4] nos CloudWatch registros deve estar ativado

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `opensearch-logs-to-cloudwatch`

Tipo de programação: acionado por alterações

Parâmetros:

- `logtype = 'error'` (não personalizável)

Esse controle verifica se os OpenSearch domínios estão configurados para enviar registros de erros para o CloudWatch Logs. Esse controle falhará se o registro de erros não CloudWatch estiver habilitado para um domínio.

Você deve ativar os registros de erros para OpenSearch domínios e enviá-los aos CloudWatch Registros para retenção e resposta. Os logs de erros do domínio podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

Correção

Para habilitar a publicação de registros, consulte Ativação da publicação de registros (console) no Amazon OpenSearch Service Developer Guide.

Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `opensearch-audit-logging-enabled`

Tipo de programação: acionado por alterações

Parâmetros:

- `cloudWatchLogsLogGroupArnList` (não personalizável): o Security Hub não preenche esse parâmetro. Lista separada por vírgulas de grupos de CloudWatch registros de registros que devem ser configurados para registros de auditoria.

Essa regra é `NON_COMPLIANT` válida se o grupo de CloudWatch registros de registros do OpenSearch domínio não estiver especificado nessa lista de parâmetros.

Esse controle verifica se os OpenSearch domínios têm o registro de auditoria ativado. Esse controle falhará se um OpenSearch domínio não tiver o registro de auditoria ativado.

Os registros em log de auditoria são altamente personalizáveis. Eles permitem que você acompanhe a atividade do usuário em seus OpenSearch clusters, incluindo sucessos e falhas de autenticação, solicitações, alterações de indexação e consultas de pesquisa recebidas. OpenSearch

Correção

Para obter instruções sobre como habilitar registros de auditoria, consulte Habilitar registros de auditoria no Amazon OpenSearch Service Developer Guide.

Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra do AWS Config : `opensearch-data-node-fault-tolerance`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os OpenSearch domínios estão configurados com pelo menos três nós de dados e `zoneAwarenessEnabled` está`true`. Esse controle falhará para um OpenSearch domínio se `instanceCount` for menor que 3 ou `zoneAwarenessEnabled` for`false`.

Um OpenSearch domínio requer pelo menos três nós de dados para alta disponibilidade e tolerância a falhas. A implantação de um OpenSearch domínio com pelo menos três nós de dados garante as operações do cluster se um nó falhar.

Correção

Para modificar o número de nós de dados em um OpenSearch domínio

1. Faça login no AWS console e abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/.
2. Em Meus domínios, escolha o nome do domínio a ser editado e escolha Editar.

3. Em Nós de dados, defina Número de nós como um número maior ou igual a 3. Para três implantações de zona de disponibilidade, defina um múltiplo de três para garantir uma distribuição igual entre as zonas de disponibilidade.
4. Selecione Enviar.

Os OpenSearch domínios [Opensearch.7] devem ter um controle de acesso refinado ativado

Requisitos relacionados: NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-11, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-12

Categoria: Proteger > Gerenciamento de acesso seguro > Ações confidenciais de API restritas

Severidade: alta

Tipo de recurso

Regra do AWS Config : `opensearch-access-control-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os OpenSearch domínios têm um controle de acesso refinado ativado. O controle falhará se o controle de acesso refinado não estiver habilitado. O controle de acesso refinado exige que `advanced-security-options` o OpenSearch parâmetro `update-domain-config` seja ativado.

O controle de acesso refinado oferece formas adicionais de controlar o acesso aos seus dados no Amazon Service. OpenSearch

Correção

Para habilitar o controle de acesso refinado, consulte Controle de acesso refinado no Amazon Service no Amazon OpenSearch Service Developer Guide. OpenSearch

[Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3),

NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de data-in-transit

Severidade: média

Tipo de recurso

Regra do AWS Config : `opensearch-https-required`

Tipo de programação: acionado por alterações

Parâmetros:

- `tlsPolicies: Policy-Min-TLS-1-2-PFS-2023-10` (não personalizável)

Isso controla se um endpoint de domínio do Amazon OpenSearch Service está configurado para usar a política de segurança TLS mais recente. O controle falhará se o endpoint do OpenSearch domínio não estiver configurado para usar a política compatível mais recente ou se o HTTPs não estiver habilitado.

O HTTPS (TLS) pode ser usado para ajudar a impedir que possíveis invasores usem ataques semelhantes para espionar person-in-the-middle ou manipular o tráfego da rede. Somente conexões criptografadas por HTTPS (TLS) devem ser permitidas. A criptografia de dados em trânsito pode afetar o desempenho. Você deve testar seu aplicativo com esse atributo para entender o perfil de desempenho e o impacto do TLS. O TLS 1.2 fornece vários aprimoramentos de segurança em relação às versões anteriores do TLS.

Correção

Para ativar a criptografia TLS, use a operação da UpdateDomainConfigAPI. Configure o DomainEndpointOptionscampo para definir `TLSSecurityPolicy` o. Para obter mais informações, consulte ode-to-node Criptografia N no Amazon OpenSearch Service Developer Guide.

Os OpenSearch domínios [Opensearch.9] devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-opensearch-domain` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um domínio do Amazon OpenSearch Service tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o domínio não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o domínio não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um domínio OpenSearch de serviço, consulte Como trabalhar com tags no Amazon OpenSearch Service Developer Guide.

Os OpenSearch domínios [Opensearch.10] devem ter a atualização de software mais recente instalada

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Detectar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `opensearch-update-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um domínio do Amazon OpenSearch Service tem a atualização de software mais recente instalada. O controle falhará se uma atualização de software estiver disponível, mas não instalada para o domínio.

OpenSearch As atualizações do software de serviço fornecem as correções, atualizações e recursos mais recentes da plataforma disponíveis para o ambiente. Manter up-to-date a instalação do patch ajuda a manter a segurança e a disponibilidade do domínio. Se você não tomar nenhuma ação sobre as atualizações necessárias, o software do serviço será atualizado automaticamente (normalmente após duas semanas). Recomendamos programar atualizações durante um período de pouco tráfego para o domínio para minimizar a interrupção do serviço.

Correção

Para instalar atualizações de software para um OpenSearch domínio, consulte Iniciando uma atualização no Amazon OpenSearch Service Developer Guide.

Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2, NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-36, Nist.800-53.r5 SI-13

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra do AWS Config : `opensearch-primary-node-fault-tolerance`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um domínio do Amazon OpenSearch Service está configurado com pelo menos três nós primários dedicados. O controle falhará se o domínio tiver menos de três nós primários dedicados.

OpenSearch O serviço usa nós primários dedicados para aumentar a estabilidade do cluster. Um nó primário dedicado executa tarefas de gerenciamento de clusters, mas não retém dados nem responde às solicitações de upload de dados. Recomendamos que você use o Multi-AZ com standby, o que adiciona três nós primários dedicados a cada domínio de produção OpenSearch .

Correção

Para alterar o número de nós primários de um OpenSearch domínio, consulte Criação e gerenciamento de domínios do Amazon OpenSearch Service no Amazon OpenSearch Service Developer Guide.

AWS Private Certificate Authority controles

Esses controles estão relacionados aos AWS Private CA recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[PCA.1] a autoridade de certificação AWS Private CA raiz deve ser desativada

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Proteger > Configuração de rede segura

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `acm-pca-root-ca-disabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se AWS Private CA tem uma autoridade de certificação raiz (CA) que está desativada. O controle falhará se a CA raiz estiver habilitada.

Com AWS Private CA, você pode criar uma hierarquia de CA que inclua uma CA raiz e CAs subordinadas. Você deve minimizar o uso da CA raiz para tarefas diárias, especialmente em ambientes de produção. A CA raiz deve ser usada apenas para emitir certificados para CAs intermediárias. Isso permite que a CA raiz seja armazenada fora de perigo, enquanto as CAs intermediárias executam a tarefa diária de emitir certificados de entidade final.

Correção

Para desabilitar a CA raiz, consulte Atualizar o status da CA no Guia do usuário do AWS Private Certificate Authority .

Amazon Relational Database Service

Esses controles estão relacionados aos recursos da API de Gateway.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[RDS.1] Os instantâneos do RDS devem ser privados

Requisitos relacionados: PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/1.3.2,PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5

AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

Categoria: Proteger > Configuração de rede segura

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `rds-snapshots-public-prohibited`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os instantâneos do RDS são públicos. O controle falhará se os instantâneos do RDS forem públicos. Esse controle avalia as instâncias do RDS, as instâncias de banco de dados do Aurora, as instâncias do banco de dados do Neptune e os clusters do Amazon DocumentDB.

Os snapshots do RDS são usados para fazer backup dos dados nas instâncias do RDS em determinado momento. Eles podem ser usados para restaurar estados anteriores das instâncias do RDS.

Um snapshot do RDS não deve ser público, a menos que isso seja o previsto. Se você compartilhar um instantâneo manual não criptografado como público, isso o disponibilizará para todas as contas da AWS. Isso pode resultar em exposição não intencional de dados da instância do RDS.

Observe que, se a configuração for alterada para permitir o acesso público, talvez a AWS Config regra não consiga detectar a alteração por até 12 horas. Até que a AWS Config regra detecte a alteração, a verificação é aprovada mesmo que a configuração viole a regra.

Para saber mais sobre como compartilhar um instantâneo de banco de dados, consulte Compartilhar um instantâneo de banco de dados no .

Correção

Para remover o acesso público dos instantâneos do RDS, consulte Compartilhamento de um instantâneo no Guia do usuário do Amazon RDS. Em DB instantâneo visibility (Visibilidade do instantâneo de banco de dados), escolha Private (Privado).

[RDS.2] As instâncias de banco de dados do RDS devem proibir o acesso público, conforme determinado pela duração PubliclyAccessible AWS Config

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.3.3, PCI DSS v3.2.1/1.2.1, PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, PCI DSS v3.2.1/7.2.1, Nist.800-53.r5 AC-4, Nist.800-53.r5 AC-4 (21), Nist.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), Nist.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-7 (5)

Categoria: Proteger > Configuração de rede segura

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `rds-instance-public-access-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se as instâncias do RDS são acessíveis publicamente avaliando o campo `PubliclyAccessible` no item de configuração da instância.

As instâncias de banco de dados Neptune e os clusters do Amazon DocumentDB não têm o sinalizador `PubliclyAccessible` e não podem ser avaliados. Entretanto, esse controle ainda pode gerar descobertas para esses recursos. É possível suprimir essas descobertas.

O valor `PubliclyAccessible` na configuração da instância do RDS indica se a instância de banco de dados é acessível publicamente. Se a instância de banco de dados for configurada com `PubliclyAccessible`, ela será uma instância voltada para a Internet com um nome de DNS que pode ser resolvido publicamente, resultando em um endereço IP público. Se a instância de banco de dados não for acessível publicamente, ela será uma instância interna com um nome de DNS que é resolvido para um endereço IP privado.

A menos que queira que a instância de RDS seja acessível publicamente, a instância de RDS não deve ser configurada com o valor `PubliclyAccessible`, pois isso pode permitir tráfego desnecessário na instância de banco de dados. Isso pode permitir tráfego desnecessário para sua instância de banco de dados.

Correção

Para remover o acesso público das instâncias de banco de dados do RDS, consulte Modificar uma instância de banco de dados do Amazon RDS no Guia do usuário do Amazon RDS. Public access (Acesso público): escolha No (Não).

[RDS.3] As instâncias de banco de dados do RDS devem ter a criptografia em repouso habilitada.

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.3.1, CIS Foundations Benchmark v1.4.0/2.3.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 AWS CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28 (1), Nist.800-53.R5 SC-7 (10), Nist.800-53.R5 SI-7 (6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra do AWS Config : `rds-storage-encrypted`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se a criptografia de armazenamento está habilitada para suas instâncias de banco de dados do RDS.

Esse controle é destinado às instâncias de banco de dados do RDS. Entretanto, ele também pode gerar descobertas para as instâncias de banco de dados do Aurora, as instâncias de banco de dados do Neptune e os clusters do Amazon DocumentDB. Se essas descobertas não forem úteis, será possível suprimi-las.

Para obter uma camada de segurança adicional para os dados confidenciais nas instâncias de banco de dados do RDS, configure as instâncias de banco de dados do RDS para serem criptografadas em repouso. Para criptografar as instâncias de banco de dados do RDS e os snapshots em repouso, habilite a opção de criptografia para as instâncias de banco de dados do RDS. Os dados criptografados em repouso incluem o armazenamento subjacente para instâncias de banco de dados, seus backups automatizados, réplicas de leitura e snapshots.

As instâncias de banco de dados criptografadas do RDS usam o algoritmo de criptografia AES-256 de padrão aberto para criptografar os dados no servidor que hospeda as instâncias de banco

de dados do RDS. Após a criptografia dos seus dados, o lida com a autenticação do acesso e a decodificação dos seus dados de forma transparente com um mínimo impacto sobre o desempenho. Você não precisa modificar seus aplicativos cliente de banco de dados para usar a criptografia.

No momento, a criptografia do Amazon RDSAmazon Aurora está disponível para todos os mecanismos de banco de dados e tipos de armazenamento. A criptografia do Amazon RDS está disponível para a maioria das classes de instância de banco de dados. Para saber mais sobre as classes de instâncias de banco de dados que não oferecem suporte para a criptografia do , consulte Criptografar recursos do no .

Correção

Para obter informações sobre criptografia de instâncias de banco de dados no Amazon RDS, consulte Criptografar recursos do Amazon RDS no Guia do usuário do Amazon RDS.

Os instantâneos do cluster do RDS e os instantâneos do banco de dados devem ser criptografados em repouso

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra do AWS Config : `rds-snapshot-encrypted`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um instantâneo do cluster de banco de dados Neptune está criptografado em repouso. O controle falhará se um instantâneo do banco de dados do RDS não estiver criptografado.

Esse controle é destinado às instâncias de banco de dados do RDS. Entretanto, ele também pode gerar descobertas para as instâncias de banco de dados do Aurora, as instâncias de banco de dados do Neptune e os clusters do Amazon DocumentDB. Se essas descobertas não forem úteis, será possível suprimi-las.

Criptografar dados em repouso reduz o risco de um usuário não autenticado ter acesso aos dados armazenados em disco. Os dados nos clusters do Amazon DocumentDB devem ser criptografados em repouso para uma camada adicional de segurança.

Correção

Para criptografar um instantâneo do RDS, consulte Criptografar recursos do Amazon RDS no Guia do usuário do Amazon RDS. Os dados criptografados em repouso incluem o armazenamento subjacente para instâncias de banco de dados, seus backups automatizados, réplicas de leitura e instantâneos.

Você só pode criptografar uma instância de banco de dados do Amazon RDS ao criá-la, e não após a criação. Entretanto, como é possível criptografar uma cópia de um snapshot não criptografado, é possível efetivamente adicionar criptografia a uma instância de banco de dados não criptografada. Ou seja, é possível criar um snapshot da sua instância de banco de dados e depois criar uma cópia criptografada desse snapshot. Em seguida, é possível restaurar uma instância de banco de dados a partir do snapshot criptografado, logo, você terá uma cópia criptografada da sua instância de banco de dados original.

As instâncias de banco de dados do RDS devem ser configuradas com várias zonas de disponibilidade

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra do AWS Config : `rds-multi-az-support`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Verifica se a alta disponibilidade está ativada para suas instâncias de banco de dados do RDS.

As instâncias de banco de dados do RDS devem ser configuradas com várias zonas de disponibilidade Isso garante a disponibilidade dos dados armazenados. As implantações Multi-AZ

permitem o failover automático se houver um problema com a disponibilidade do AZ e durante a manutenção regular do RDS.

Correção

Para implantar suas instâncias de banco de dados em várias AZs, Modificar uma instância de banco de dados para ser uma implantação de instância de banco de dados multi-AZ no Guia do usuário do Amazon RDS.

O monitoramento aprimorado deve ser configurado para instâncias de banco de dados do RDS

Requisitos relacionados: NIST.800-53.r5 SI-4 (12), NIST.800-53.r5 SI-4 (5)

Categoria: Detectar > Serviços de detecção

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `rds-enhanced-monitoring-enabled`

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub	
`monitoringInterval`	Número de segundos entre os intervalos de coleta de métricas de monitoramento	Enum	`1`, `5`, `10`, `15`, `30`, `60`	Nenhum valor padrão	

Esse controle verifica se o monitoramento aprimorado está habilitado para uma instância de banco de dados do Amazon Relational Database Service (Amazon RDS). O controle falhará se o monitoramento aprimorado não estiver habilitado para a instância. Se você fornecer um valor

personalizado para o parâmetro `monitoringInterval`, o controle será aprovado somente se as métricas de monitoramento aprimorado forem coletadas para a instância no intervalo especificado.

No Amazon RDS, o monitoramento aprimorado permite uma resposta mais rápida às alterações de desempenho na infraestrutura subjacente. Mudanças no desempenho podem resultar na falta de disponibilidade da API. O monitoramento aprimorado do Amazon RDS fornece métricas em tempo real para o sistema operacional (SO) no qual a instância do banco de dados é executada. O agente do está instalado e em execução na instância? O agente pode obter métricas com mais precisão do que é possível na camada do hipervisor.

As métricas de Monitoramento avançado são úteis quando você deseja ver como os diferentes processos ou threads em uma instância de banco de dados usam a CPU. Para obter mais informações, consulte Monitoramento avançado no Guia do usuário do Amazon RDS.

Correção

Para obter instruções detalhadas sobre como habilitar o monitoramento aprimorado para sua instância de banco de dados, consulte Configurar e ativar o monitoramento aprimorado no Guia do usuário do Amazon RDS.

[RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Proteger > Proteção de dados > Proteção contra exclusão de dados

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `rds-cluster-deletion-protection-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster do Amazon DocumentDB tem a proteção contra exclusão habilitada. O controle falhará se o cluster não tiver a proteção contra exclusão habilitada.

Esse controle é destinado às instâncias de banco de dados do RDS. Entretanto, ele também pode gerar descobertas para as instâncias de banco de dados do Aurora, as instâncias de banco de dados

do Neptune e os clusters do Amazon DocumentDB. Se essas descobertas não forem úteis, será possível suprimi-las.

A ativação da proteção contra exclusão de clusters oferece uma camada adicional de proteção contra a exclusão acidental do banco de dados ou a exclusão por um usuário não autorizado.

O cluster de banco de dados não poderá ser excluído se a proteção contra exclusão estiver ativada. Primeiro, você deve desativar a proteção contra exclusão para que uma solicitação de exclusão possa ser bem-sucedida.

Correção

Para ativar a proteção contra exclusão de um cluster de banco de dados Neptune existente, consulte Modificar o cluster de banco de dados usando o console, a CLI e a API no Guia do usuário do Amazon Aurora. Para Deletion protection (Proteção contra exclusão), escolha Enable deletion protection (Habilitar proteção contra exclusão).

[RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Proteger > Proteção de dados > Proteção contra exclusão de dados

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `rds-instance-deletion-protection-enabled`

Tipo de programação: acionado por alterações

Parâmetros:

- `databaseEngines`: `mariadb,mysql,custom-oracle-ee,oracle-ee-cdb,oracle-se2-cdb,oracle-ee,oracle-se2,oracle-se1,oracle-se,postgres,sqlserver-ee,sqlserver-se,sqlserver-ex,sqlserver-web` (não personalizável)

Esse controle verifica se suas instâncias de banco de dados do RDS que usam um dos mecanismos de banco de dados listados têm a proteção contra exclusão ativada. O controle falhará se o cluster não tiver a proteção contra exclusão habilitada.

A ativação da proteção contra exclusão de clusters oferece uma camada adicional de proteção contra a exclusão acidental do banco de dados ou a exclusão por um usuário não autorizado.

Embora a proteção contra exclusão esteja ativada, uma instância de banco de dados do RDS não pode ser excluída. Primeiro, você deve desativar a proteção contra exclusão para que uma solicitação de exclusão possa ser bem-sucedida.

Correção

Para ativar a proteção contra exclusão de uma instância de banco de dados do RDS, consulte Modificar uma instância de banco de dados do Amazon RDS no Guia do usuário do Amazon RDS. Para Deletion protection (Proteção contra exclusão), escolha Enable deletion protection (Habilitar proteção contra exclusão).

[RDS.9] As instâncias de banco de dados do RDS devem publicar registros no Logs CloudWatch

Requisitos relacionados: CIS Foundations Benchmark v1.2.0/2.1, CIS Foundations Benchmark v1.4.0/3.1, NIST.800-53.r5 AC-2(4), NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AC-6(9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 AU-14(1), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-3(8), NIST.800-53.r5 SI-4(20), NIST.800-53.r5 SI-7(8), NIST.800-53.r5 SA-8(22)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `rds-logging-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma instância de banco de dados Amazon RDS está configurada para publicar os seguintes registros no Amazon CloudWatch Logs. O controle falhará se a instância não estiver configurada para publicar os seguintes registros no CloudWatch Logs:

- Oracle: (Alert, Audit, Trace, Listener)

- PostgreSQL: (Postgresql, Upgrade)
- MySQL: (Auditoria, Erro, Geral,) SlowQuery
- MariaDB: (Auditoria, erro, geral) SlowQuery
- SQL Server: (Error, Agent)
- Aurora: (Auditoria, erro, geral) SlowQuery
- Aurora-MySQL: (Auditoria, Erro, Geral,) SlowQuery
- Aurora-PostgreSQL: (Postgresql, Upgrade).

Os bancos de dados do RDS devem ter os registros relevantes habilitados. O registro em log do banco de dados fornece registros detalhados das solicitações feitas ao RDS. Os logs de erros do domínio podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

Correção

Para publicar registros do banco de dados do RDS no CloudWatch Logs, consulte Especificação dos registros a serem publicados nos CloudWatch Logs no Guia do usuário do Amazon RDS.

A autenticação do IAM deve ser configurada para instâncias do RDS

Requisitos relacionados: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6

Categoria: Proteger > Gerenciamento de acesso seguro > Autenticação sem senha

Severidade: média

Tipo de recurso

Regra do AWS Config : `rds-instance-iam-authentication-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma instância de banco de dados do RDS tem a autenticação de banco de dados do IAM ativada. O controle falhará se a autenticação do IAM não estiver configurada para instâncias de banco de dados do RDS. Esse controle avalia somente instâncias do RDS com os seguintes tipos de mecanismo: `mysql`, `postgres`, `aurora`, `aurora-mysql`, `aurora-`

`postgresql` e `mariadb`. Uma instância do RDS também deve estar em um dos seguintes estados para que uma descoberta seja gerada: `available`, `backing-up`, `storage-optimization` ou `storage-full`.

A autenticação de banco de dados do IAM permite a autenticação em instâncias de banco de dados com um token de autenticação em vez de uma senha. O tráfego de rede de e para o banco de dados é criptografado usando o Secure Sockets Layer (SSL). Para obter mais informações, consulte Autenticação de banco de dados do IAM no Guia do usuário do Amazon Aurora.

Correção

Para ativar a autenticação do banco de dados do IAM em uma instância de banco de dados do RDS, consulte Habilitar e desabilitar a autenticação do banco de dados do IAM no Guia do usuário do Amazon RDS.

As instâncias do RDS devem ter backups automáticos habilitados

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Recuperação > Resiliência > Backups ativados

Severidade: média

Tipo de recurso

Regra do AWS Config : `db-instance-backup-enabled`

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub	
`backupRetentionMinimum`	Período mínimo de retenção de backups em dias	Inteiro	7 para 35	7	

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub	
`checkReadReplicas`	Verifica se as instâncias de banco de dados do RDS têm backups habilitados para réplicas de leitura	Booleano	Não personalizável	`false`	

Esse controle verifica se uma instância do Amazon Relational Database Service têm backups automatizados habilitados e se o período de retenção de backups é maior ou igual ao período de tempo especificado. As réplicas de leitura são excluídas da avaliação. O controle falhará se os backups não estiverem habilitados para a instância, ou se o período de retenção for inferior ao período de tempo especificado. A menos que você forneça um valor de parâmetro personalizado para o período de retenção do backup, o Security Hub usará um valor padrão de 7 dias.

Os backups ajudam você a se recuperar mais rapidamente de um incidente de segurança e a fortalecer a resiliência de seus sistemas. O Amazon RDS permite que você configure snapshots diários do volume completo da instância. Para obter mais informações sobre backups automatizados do Amazon RDS, consulte Trabalho com backups no Guia do usuário do Amazon RDS.

Correção

Para obter instruções sobre como habilitar backups automatizados para uma instância de banco de dados do RDS for PostgreSQL, consulte Enabling automated backups (Habilitar backups automatizados) no Manual do usuário da Amazon RDS.

A autenticação do IAM deve ser configurada para instâncias do RDS

Requisitos relacionados: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6

Categoria: Proteger > Gerenciamento de acesso seguro > Autenticação sem senha

Severidade: média

Tipo de recurso

Regra do AWS Config : `rds-cluster-iam-authentication-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma instância de banco de dados do RDS tem a autenticação de banco de dados do IAM ativada.

A autenticação de banco de dados do IAM permite a autenticação sem senha para instâncias de banco de dados. A autenticação usa um token de autenticação. O tráfego de rede de e para o banco de dados é criptografado usando o Secure Sockets Layer (SSL). Para obter mais informações, consulte Autenticação de banco de dados do IAM no Guia do usuário do Amazon Aurora.

Correção

Para ativar a autenticação do banco de dados do IAM em uma instância de banco de dados do RDS, consulte Habilitar e desabilitar a autenticação do banco de dados do IAM no Guia do usuário do Amazon RDS.

[RDS.13] As atualizações automáticas de versões secundárias do RDS devem ser ativadas

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.3.2, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5)

Categoria: Detectar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: alta

Tipo de recurso

Regra do AWS Config : `rds-automatic-minor-version-upgrade-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se as atualizações automáticas de versões secundárias estão habilitadas para a instância do banco de dados do RDS.

A ativação de atualizações automáticas de versões secundárias garante que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) sejam instaladas. incluem os patches de segurança e as correções de erros mais recentes. Manter-se atualizado com a instalação do patch é uma etapa importante para proteger os sistemas.

Correção

Para habilitar atualizações automáticas de versões secundárias para uma instância de banco de dados existente, consulte Modificar uma instância de banco de dados Amazon RDS no Guia do usuário do Amazon RDS. Em Atualização automática da versão secundária, selecione Sim.

[RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado

Requisitos relacionados: NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-11, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-12

Categoria: Recuperação > Resiliência > Backups ativados

Severidade: média

Tipo de recurso

Regra do AWS Config : `aurora-mysql-backtracking-enabled`

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub	
`BacktrackWindowInHours`	Número de horas para retroceder um cluster do Aurora MySQL	Double	`0.1` para `72`	Nenhum valor padrão	

Esse controle verifica se um cluster do Amazon Aurora têm o retrocesso habilitado. O controle falhará se o cluster não tiver o retrocesso habilitado. Se você fornecer um valor personalizado para

o parâmetro `BacktrackWindowInHours`, o controle passará somente se o cluster for retrocedido pelo período de tempo especificado.

Os backups ajudam você a se recuperar mais rapidamente de um incidente de segurança. Eles também fortalecem a resiliência de seus sistemas. O backtracking do Aurora reduz o tempo de recuperação de um banco de dados para um ponto no tempo. Não é necessária uma restauração do banco de dados para fazer isso.

Correção

Para habilitar o retrocesso do Aurora, consulte Configuração do retrocesso no Guia do usuário do Amazon Aurora.

Observe que você não pode ativar o backtracking em um cluster existente. Em vez disso, é possível criar um clone com o backtracking habilitado. Para obter mais informações sobre as limitações do backtracking do Aurora, consulte a lista de limitações em Visão geral do backtracking.

[RDS.15] Os clusters de banco de dados do RDS devem ser configurados para várias zonas de disponibilidade

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra do AWS Config : `rds-cluster-multi-az-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Verifica se a alta disponibilidade está ativada para suas instâncias de banco de dados do RDS. O controle falhará se um cluster de banco de dados do RDS não for implantado em várias Zonas de disponibilidade (AZs).

Os clusters de banco de dados do RDS devem ser configurados para várias AZs para garantir a disponibilidade dos dados armazenados. A implantação em várias AZs permite o failover

automatizado no caso de um problema de disponibilidade do AZ e durante eventos regulares de manutenção do RDS.

Correção

Para implantar suas instâncias de banco de dados em várias AZs, Modificar uma instância de banco de dados para ser uma implantação de instância de banco de dados multi-AZ no Guia do usuário do Amazon RDS.

As etapas de correção são diferentes nos bancos de dados globais do Aurora. Para configurar várias zonas de disponibilidade para um banco de dados global do Aurora, selecione seu cluster de banco de dados. Em seguida, escolha Ações e Adicionar leitor e especifique várias AZs. Para obter mais informações, consulte Gerenciar um cluster de banco de dados do Amazon Aurora no Guia do usuário do Amazon Aurora.

Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `rds-cluster-copy-tags-to-snapshots-enabled` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster de banco de dados Neptune está configurado para copiar todas as tags para instantâneos quando os instantâneos são criados.

A identificação de seus ativos de TI é um aspecto essencial de governança e segurança. Para avaliar seus procedimentos de segurança e atuar em possíveis pontos fracos, é necessário ter visibilidade de todos os seus buckets do . Você deve marcar instantâneos da mesma forma que os clusters de banco de dados do Amazon RDS primário. A ativação dessa configuração garante que os instantâneos herdem as tags de seus clusters de banco de dados principais.

Correção

Para copiar automaticamente tags para instantâneos de um cluster de banco de dados do RDS, consulte Modificar cluster de banco de dados usando o console, a CLI e a API no Guia do usuário do Amazon Aurora. Copiar tags para instantâneos

As instâncias de banco de dados do RDS devem ser configuradas para copiar tags para instantâneos

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `rds-instance-copy-tags-to-snapshots-enabled` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster de banco de dados Neptune está configurado para copiar todas as tags para instantâneos quando os instantâneos são criados.

A identificação de seus ativos de TI é um aspecto essencial de governança e segurança. É necessário ter visibilidade de seus recursos do para avaliar sua postura de segurança e agir em possíveis áreas de fraqueza. Você deve marcar instantâneos da mesma forma que os clusters de banco de dados do Amazon RDS primário. A ativação dessa configuração garante que os instantâneos herdem as tags de seus clusters de banco de dados principais.

Correção

Para copiar automaticamente as tags para instantâneos de uma instância de banco de dados do RDS, consulte Modificar uma instância de banco de dados do Amazon RDS no Guia do usuário do Amazon RDS. Copiar tags para instantâneos

As instâncias do RDS devem ser implantadas em uma VPC

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3),

NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso

Regra AWS Config : `rds-deployed-in-vpc` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma instância do Amazon RDS está implantada em uma EC2-VPC.

As VPCs fornecem vários controles de rede para proteger o acesso aos recursos do RDS. Esses controles incluem endpoints da VPC, ACLs de rede e grupos de segurança. Para aproveitar esses controles, recomendamos que você crie suas instâncias do RDS em uma EC2-VPC.

Correção

Para obter instruções sobre como mover instâncias do RDS para uma VPC, consulte Atualizar a VPC para uma instância de banco de dados no Guia do usuário do Amazon RDS.

As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de cluster

Requisitos relacionados: NIST.800-53.r5 SI-4 (12), NIST.800-53.r5 SI-4 (5)

Categoria: Detectar > Serviços de detecção > Monitoramento de aplicativos

Severidade: baixa

Tipo de recurso

Regra AWS Config : `rds-cluster-event-notifications-configured` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma assinatura de eventos existente do Amazon RDS para clusters de banco de dados tem notificações habilitadas para os seguintes pares de valores-chave de tipo de fonte e categoria de evento:

```
DBCluster: ["maintenance","failure"]
```

O controle é aprovado se não houver assinaturas de eventos existentes em sua conta.

As notificações de eventos do RDS usam o Amazon SNS para informá-lo sobre alterações na disponibilidade ou na configuração dos seus recursos do RDS. Essas notificações permitem uma resposta rápida. Para obter mais informações, consulte Usar a notificação de evento do Amazon RDS no Manual do usuário do Amazon RDS.

Correção

Para assinar notificações de eventos de cluster do RDS, consulte Assinatura da notificação de eventos do Amazon RDS no Guia do usuário do Amazon RDS. Use os seguintes valores:

Campo	Valor
Tipo de origem	Clusters
Clusters a serem incluídos	Todos os clusters
Categorias de eventos a serem incluídas	Selecione categorias de eventos específicas ou Todas as categorias de eventos

As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de cluster

Requisitos relacionados: NIST.800-53.r5 SI-4 (12), NIST.800-53.r5 SI-4 (5)

Categoria: Detectar > Serviços de detecção > Monitoramento de aplicativos

Severidade: baixa

Tipo de recurso

Regra AWS Config : `rds-instance-event-notifications-configured` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma assinatura de eventos existente do Amazon RDS para clusters de banco de dados tem notificações habilitadas para os seguintes pares de valores-chave de tipo de fonte e categoria de evento:

```
DBInstance: ["maintenance","configuration change","failure"]
```

O controle é aprovado se não houver assinaturas de eventos existentes em sua conta.

As notificações de eventos do RDS usam o Amazon SNS para informá-lo sobre mudanças na disponibilidade ou na configuração dos seus recursos do RDS. Essas notificações permitem uma resposta rápida. Para obter mais informações, consulte Usar a notificação de evento do Amazon RDS no Manual do usuário do Amazon RDS.

Correção

Para assinar notificações de eventos de cluster do RDS, consulte Assinatura da notificação de eventos do Amazon RDS no Guia do usuário do Amazon RDS. Use os seguintes valores:

Campo	Valor
Tipo de origem	Instâncias
Instâncias a serem incluídas	Todas as instâncias
Categorias de eventos a serem incluídas	Selecione categorias de eventos específicas ou Todas as categorias de eventos

Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de parâmetros do banco de dados

Requisitos relacionados: NIST.800-53.r5 SI-4 (12), NIST.800-53.r5 SI-4 (5)

Categoria: Detectar > Serviços de detecção > Monitoramento de aplicativos

Severidade: baixa

Tipo de recurso

Regra AWS Config : `rds-pg-event-notifications-configured` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma assinatura de eventos existente do Amazon RDS para clusters de banco de dados tem notificações habilitadas para os seguintes pares de valores-chave de tipo de fonte e categoria de evento:

```
DBParameterGroup: ["configuration change"]
```

As notificações de eventos do RDS usam o Amazon SNS para informá-lo sobre mudanças na disponibilidade ou na configuração dos seus recursos do RDS. Essas notificações permitem uma resposta rápida. Para obter mais informações, consulte Usar a notificação de evento do Amazon RDS no Manual do usuário do Amazon RDS.

Correção

Para assinar notificações de eventos de cluster do RDS, consulte Assinatura da notificação de eventos do Amazon RDS no Guia do usuário do Amazon RDS. Use os seguintes valores:

Campo	Valor
Tipo de origem	Grupos de parâmetros
Grupos de parâmetros a serem incluídos	Grupos de parâmetros
Categorias de eventos a serem incluídas	Selecione categorias de eventos específicas ou Todas as categorias de eventos

Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do grupo de parâmetros do banco de dados

Requisitos relacionados: NIST.800-53.r5 SI-4 (12), NIST.800-53.r5 SI-4 (5)

Categoria: Detectar > Serviços de detecção > Monitoramento de aplicativos

Severidade: baixa

Tipo de recurso

Regra AWS Config : `rds-sg-event-notifications-configured` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma assinatura de eventos existente do Amazon RDS para clusters de banco de dados tem notificações habilitadas para os seguintes pares de valores-chave de tipo de fonte e categoria de evento:

```
DBSecurityGroup: ["configuration change","failure"]
```

As notificações de eventos do RDS usam o Amazon SNS para informá-lo sobre mudanças na disponibilidade ou na configuração dos seus recursos do RDS. Essas notificações permitem uma resposta rápida. Para obter mais informações, consulte Usar a notificação de evento do Amazon RDS no Manual do usuário do Amazon RDS.

Correção

Para assinar notificações de eventos de cluster do RDS, consulte Assinatura da notificação de eventos do Amazon RDS no Guia do usuário do Amazon RDS. Use os seguintes valores:

Campo	Valor
Tipo de origem	Grupos de segurança
Grupos de segurança a serem incluídos	Grupos de segurança de banco de dados
Categorias de eventos a serem incluídas	Selecione categorias de eventos específicas ou Todas as categorias de eventos

As instâncias do RDS não devem usar uma porta padrão do mecanismo de banco de dados

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Configuração de rede segura

Severidade: baixa

Tipo de recurso

Regra AWS Config : `rds-no-default-ports` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster ou instância do RDS usa uma porta diferente da porta padrão do mecanismo de banco de dados. O controle falhará se o cluster ou a instância do RDS usar a porta padrão.

Se você usar uma porta conhecida para implantar um cluster ou instância do RDS, um invasor poderá adivinhar informações sobre o cluster ou a instância. O invasor pode usar essas informações em conjunto com outras informações para se conectar a um cluster ou instância do RDS ou obter informações adicionais sobre seu aplicativo.

Ao alterar a porta, você também deve atualizar as cadeias de conexão existentes que foram usadas para se conectar à porta antiga. Você também deve verificar o grupo de segurança da instância de banco de dados para garantir que ele inclua uma regra de entrada que permita conectividade na nova porta.

Correção

Para modificar a porta padrão de uma instância de banco de dados RDS existente, consulte Modificar uma instância de banco de dados Amazon RDS no Guia do usuário do Amazon RDS. Para ativar a proteção contra exclusão de um cluster de banco de dados Neptune existente, consulte Modificar o cluster de banco de dados usando o console, a CLI e a API no Guia do usuário do Amazon Aurora. Em Porta do banco de dados, altere o valor da porta para um valor não padrão.

Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Configuração de recursos

Severidade: média

Tipo de recurso

Regra do AWS Config : `rds-cluster-default-admin-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster de banco de dados do Amazon RDS alterou o nome de usuário do administrador de seu valor padrão. O controle não se aplica a mecanismos do tipo neptune (Neptune DB) ou docdb (DocumentDB). Essa regra falhará se o nome de usuário do administrador estiver definido com o valor padrão.

Ao criar um banco de dados do Amazon RDS, você deve alterar o nome de usuário do administrador padrão para um valor exclusivo. Os nomes de usuário padrão são de conhecimento público e devem ser alterados durante a criação do banco de dados RDS. Alterar os nomes de usuário padrão reduz o risco de acesso não intencional.

Correção

Para alterar o nome de usuário do administrador associado ao cluster de banco de dados do Amazon RDS, crie um novo cluster de banco de dados do RDS e altere o nome de usuário do administrador padrão ao criar o banco de dados.

Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Configuração de recursos

Severidade: média

Tipo de recurso

Regra do AWS Config : `rds-instance-default-admin-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se você alterou o nome de usuário administrativo para as instâncias de banco de dados do Amazon Relational Database Service (Amazon RDS) do valor padrão do nome de usuário administrativo para as instâncias de banco de dados do Amazon Relational Database

Service (Amazon RDS). O controle não se aplica a mecanismos do tipo neptune (Neptune DB) ou docdb (DocumentDB). Essa regra falhará se o nome de usuário do administrador estiver definido com o valor padrão.

Os nomes de usuário administrativos padrão nos bancos de dados do Amazon RDS são de conhecimento público. Ao criar um banco de dados do Amazon RDS, você deve alterar o nome de usuário do administrador padrão para um valor exclusivo.

Correção

Para alterar o nome de usuário administrativo associado a uma instância do banco de dados do RDS, primeiro crie uma nova instância do banco de dados do RDS. Altere o nome de usuário administrativo padrão ao criar o banco de dados.

As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup

Categoria: Recuperação > Resiliência > Backups ativados

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Severidade: média

Tipo de recurso

AWS Config regra: **`rds-resources-protected-by-backup-plan`**

Tipo de programação: Periódico

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub	
`backupVaultLockCheck`	O controle produz uma `PASSED` descoberta se o parâmetro estiver definido como verdadeir	Booleano	`true` ou `false`	Nenhum valor padrão	

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub	
	o e o recurso usar o AWS Backup Vault Lock.				

Esse controle avalia se as instâncias de banco de dados do Amazon RDS estão cobertas por um plano de backup. Esse controle falhará se a instância de banco de dados do RDS não estiver coberta por um plano de backup. Se você definir o `backupVaultLockCheck` parâmetro igual `atrue`, o controle passará somente se o backup da instância for feito em um cofre AWS Backup bloqueado.

AWS Backup é um serviço de backup totalmente gerenciado que centraliza e automatiza o backup dos dados. Serviços da AWS Com AWS Backup, você pode criar políticas de backup chamadas planos de backup. É possível usar esses planos para definir seus requisitos de backup, como a frequência com a qual fazer o backup de seus dados e por quanto tempo manter esses backups. Incluir tabelas do DynamoDB em seus planos de backup ajuda a proteger seus dados contra perda ou exclusão não intencionais.

Correção

Para adicionar uma instância de banco de dados do RDS a um plano de AWS Backup backup, consulte Atribuição de recursos a um plano de backup no Guia do AWS Backup desenvolvedor.

Os clusters de banco de dados Neptune devem ser criptografados em repouso

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

AWS Config regra: **`rds-cluster-encrypted-at-rest`**

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster do Amazon DocumentDB é criptografado em repouso. O controle falhará se um cluster de banco de dados Neptune não estiver criptografado em repouso.

Dados em repouso se referem a qualquer dado armazenado em armazenamento persistente e não volátil por qualquer período. A criptografia ajuda a proteger a confidencialidade desses dados, reduzindo o risco de que um usuário não autorizado possa acessá-los. Criptografar seus clusters de banco de dados Neptune protege seus dados e metadados contra acesso não autorizado. Ele também atende aos requisitos de conformidade para data-at-rest criptografia de sistemas de arquivos de produção.

Correção

É possível ativar a criptografia em repouso ao criar um cluster do RDS DB. Não é possível alterar as configurações de criptografia após a criação de um cluster. Para obter mais informações, consulte Gerenciar um cluster de banco de dados do Amazon Aurora no Guia do usuário do Amazon Aurora.

[RDS.28] Os clusters de banco de dados do RDS devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

AWS Config regra: `tagged-rds-dbcluster` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um cluster de banco de dados do Amazon RDS tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o cluster de banco de dados não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o cluster de banco de dados não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um cluster de banco de dados do RDS, consulte Como marcar recursos do Amazon RDS no Guia do usuário do Amazon RDS.

[RDS.29] Os instantâneos do cluster de banco de dados do RDS devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

AWS Config regra: `tagged-rds-dbclustersnapshot` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um snapshot de cluster de banco de dados do Amazon RDS tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o snapshot do cluster de banco de dados não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o snapshot do cluster de banco de dados não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um snapshot de cluster de banco de dados do RDS, consulte Como marcar recursos do Amazon RDS no Guia do usuário do Amazon RDS.

[RDS.30] As instâncias de banco de dados do RDS devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

AWS Config regra: `tagged-rds-dbinstance` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se uma instância de banco de dados Amazon RDS tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a instância de banco de dados não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a instância de banco de dados não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma instância de banco de dados do RDS, consulte Como marcar recursos do Amazon RDS no Guia do usuário do Amazon RDS.

[RDS.31] Os grupos de segurança do RDS DB devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

AWS Config regra: `tagged-rds-dbsecuritygroup` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um grupo de segurança de banco de dados do Amazon RDS tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o grupo de segurança do banco de dados não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o grupo de segurança do banco de dados não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um grupo de segurança do banco de dados do RDS, consulte Como marcar recursos do Amazon RDS no Guia do usuário do Amazon RDS.

[RDS.32] Os instantâneos do banco de dados do RDS devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

AWS Config regra: `tagged-rds-dbsnapshot` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um DB snapshot do Amazon RDS tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o DB snapshot não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o DB snapshot não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um DB snapshot do RDS, consulte Como marcar recursos do Amazon RDS no Guia do usuário do Amazon RDS.

[RDS.33] Os grupos de sub-redes do banco de dados do RDS devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

AWS Config regra: `tagged-rds-dbsubnetgroups` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um grupo de sub-redes de banco de dados do Amazon RDS tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o grupo de sub-redes do banco de dados não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o grupo de sub-redes do banco de dados não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um grupo de sub-redes de banco de dados do RDS, consulte Como marcar recursos do Amazon RDS no Guia do usuário do Amazon RDS.

[RDS.34] Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

AWS Config regra: **`rds-aurora-mysql-audit-logging-enabled`**

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster de banco de dados Amazon Aurora MySQL está configurado para publicar logs de auditoria no Amazon Logs. CloudWatch O controle falhará se o cluster não estiver configurado para publicar registros de auditoria no CloudWatch Logs.

Os logs de auditoria capturam um registro da atividade do banco de dados, incluindo tentativas de login, modificações de dados, alterações de esquema e outros eventos que podem ser auditados para fins de segurança e conformidade. Ao configurar um cluster de banco de dados Aurora MySQL para publicar registros de auditoria em um grupo de logs no Amazon CloudWatch Logs, você pode realizar análises em tempo real dos dados de log. CloudWatch O Logs retém os registros em um

armazenamento altamente durável. Você também pode criar alarmes e visualizar métricas no CloudWatch.

> **Note**
>
> Uma forma alternativa de publicar registros de auditoria no Logs é habilitar a auditoria avançada e definir o parâmetro de banco de CloudWatch dados em nível de cluster como. `server_audit_logs_upload` `1` O padrão para `server_audit_logs_upload` `parameter` é `0`. Entretanto, recomendamos que você use as seguintes instruções de correção para passar esse controle.

Correção

Para publicar registros de auditoria do cluster de banco de dados Aurora MySQL no Logs, consulte Publicação de CloudWatch registros do Amazon Aurora MySQL no Amazon Logs CloudWatch no Guia do usuário do Amazon Aurora.

Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Detectar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: média

Tipo de recurso

AWS Config regra: **`rds-cluster-auto-minor-version-upgrade-enable`**

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se a atualização automática de versões secundárias está habilitada para um cluster de banco de dados Amazon RDS Multi-AZ. O controle falhará se a atualização automática de versões secundárias não estiver habilitada para o cluster de banco de dados Multi-AZ.

O RDS fornece atualização automática de versões secundárias para que você possa manter seu cluster de banco de dados Multi-AZ atualizado. Versões secundárias podem introduzir novos

atributos de software, correções de bugs, patches de segurança e melhorias de desempenho. Ao habilitar a atualização automática de versões secundárias em clusters de banco de dados do RDS, o cluster, junto com as instâncias no cluster, receberá atualizações automáticas para a versão secundária quando novas versões estiverem disponíveis. As atualizações são aplicadas durante o período de manutenção.

Correção

Para habilitar a atualização automática de versões secundárias em clusters de banco de dados Multi-AZ, consulte Modificação de um cluster de banco de dados Multi-AZ no Guia do usuário do Amazon RDS.

COPY do Amazon Redshift

Esses controles estão relacionados aos recursos do Amazon DocumentDB.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[PCI.Redshift.1] Os clusters do devem proibir o acesso público

Requisitos relacionados: PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/1.3.2,PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

Categoria: Proteger > Configuração de rede segura > Recursos não acessíveis ao público

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `redshift-cluster-public-access-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um endpoint de cluster Amazon EKS está acessível publicamente. Ele avalia o campo `PubliclyAccessible` no item de configuração do cluster.

O atributo `PubliclyAccessible` da configuração do cluster do Amazon Redshift indica se o cluster está acessível publicamente. Se a instância de banco de dados for configurada com , ela será uma instância voltada para a Internet com um nome de DNS que pode ser resolvido publicamente, resultando em um endereço IP público.

Se a instância de banco de dados não for acessível publicamente, ela será uma instância interna com um nome de DNS que é resolvido para um endereço IP privado. A menos que você pretenda que seu cluster seja acessível publicamente, o cluster não deve ser configurado com `PubliclyAccessible` definido como `true`.

Correção

Para atualizar um cluster do Amazon Redshift para desativar o acesso público, consulte Modificar um cluster no Guia de gerenciamento do Amazon Redshift. Defina Publicly accessible (Acessível ao público) como Yes (Sim).

As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em trânsito

Severidade: média

Tipo de recurso: `AWS::Redshift::Cluster` `AWS::Redshift::ClusterParameterGroup`

Regra do AWS Config : `redshift-require-tls-ssl`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se as conexões com os clusters do Amazon Redshift são necessárias para usar criptografia em trânsito. A verificação falhará se o parâmetro de cluster do Amazon Redshift `require_SSL` não estiver definido como `True`.

O TLS pode ser usado para ajudar a impedir que possíveis invasores usem ataques semelhantes para espionar person-in-the-middle ou manipular o tráfego da rede. Somente conexões criptografadas via TLS devem ser permitidas. A criptografia de dados em trânsito pode afetar

o desempenho. Você deve testar seu aplicativo com esse atributo para entender o perfil de desempenho e o impacto do TLS.

Correção

Para atualizar um grupo de parâmetros do Amazon Redshift para exigir criptografia, consulte Modificar um grupo de parâmetros no Guia de gerenciamento do Amazon Redshift. Defina como verdadeiro.

Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Recuperação > Resiliência > Backups ativados

Severidade: média

Tipo de recurso

Regra do AWS Config : `redshift-backup-enabled`

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub	
`MinRetentionPeriod`	Período mínimo de retenção de snapshot em dias	Inteiro	`7` para `35`	`7`	

Esse controle verifica se um cluster do Amazon Redshift tem snapshots automatizados habilitados e um período de retenção maior ou igual ao período de tempo especificado. O controle falhará se os snapshots automatizados não estiverem habilitados para o cluster, ou se o período de retenção for inferior ao período de tempo especificado. A menos que você forneça um valor de parâmetro

personalizado para o período de retenção do snapshot, o Security Hub usará um valor padrão de 7 dias.

Os backups ajudam você a se recuperar mais rapidamente de um incidente de segurança. Eles também fortalecem a resiliência de seus sistemas. O Amazon Redshift faz instantâneos periódicos por padrão. Esse controle verifica se os instantâneos automáticos estão habilitados e retidos por pelo menos sete dias. Para obter mais detalhes sobre os instantâneos automatizados do Amazon Redshift, consulte instantâneos automatizados no Guia de gerenciamento do Amazon Redshift.

Correção

Para atualizar o período de retenção de instantâneos para um cluster do Amazon Redshift, consulte Modificar um cluster no Guia de gerenciamento do Amazon Redshift. Em Backup, defina Retenção de instantâneos para um valor de 7 ou mais.

Os clusters do Amazon Redshift devem ter o registro de auditoria ativado

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra AWS Config : `redshift-cluster-audit-logging-enabled` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

- `loggingEnabled = true` (não personalizável)

Esse controle verifica se um cluster de banco de dados Amazon Aurora MySQL tem log de auditoria habilitado.

O registro em log de auditoria do Amazon Redshift fornece informações adicionais sobre conexões e atividades do usuário em seu cluster. Esses dados podem ser armazenados e protegidos no Amazon

S3 e podem ser úteis em auditorias e investigações de segurança. Para obter mais informações, consulte “Carregar dados do Amazon S3” no Guia de gerenciamento de clusters do Amazon Redshift.

Correção

Para configurar o registro de auditoria para um cluster do Amazon Redshift, consulte Configurar auditoria usando o console no Guia de gerenciamento do Amazon Redshift.

O Amazon Redshift deve ter as atualizações automáticas para as versões principais habilitadas

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Detectar > Gerenciamento de vulnerabilidades, patches e versões

Severidade: média

Tipo de recurso

Regra do AWS Config : `redshift-cluster-maintenancesettings-check`

Tipo de programação: acionado por alterações

Parâmetros:

- `allowVersionUpgrade = true` (não personalizável)

Esse controle verifica se as atualizações automáticas de versões principais estão habilitadas para o cluster Amazon Redshift.

A ativação de atualizações automáticas de versões principais garante que as atualizações mais recentes da versão principal dos clusters do Amazon Redshift sejam instaladas durante a janela de manutenção. incluem os patches de segurança e as correções de erros mais recentes. Manter-se atualizado com a instalação do patch é uma etapa importante para proteger os sistemas.

Correção

Para corrigir esse problema a partir do AWS CLI, use o comando Amazon `modify-cluster` Redshift para definir `--allow-version-upgrade` o atributo.

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

onde *clustername* é o nome do cluster do Amazon EKS.

Os clusters do Redshift devem usar roteamento de VPC aprimorado

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso

Regra do AWS Config : `redshift-enhanced-vpc-routing-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster do Amazon Redshift foi `EnhancedVpcRouting` ativado.

Use o roteamento aprimorado de VPC com o `COPY` para forçar todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados pela `UNLOAD`. Em seguida, é possível usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar logs de fluxo da VPC para monitorar o tráfego de rede.

Correção

Para obter instruções detalhadas de correção, consulte Ativar roteamento aprimorado de VPC no Guia de gerenciamento do Amazon Redshift.

Os clusters do Amazon Redshift não devem usar o nome de usuário Admin padrão

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Configuração de recursos

Severidade: média

Tipo de recurso

Regra do AWS Config : `redshift-default-admin-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster de banco de dados do Amazon RDS alterou o nome de usuário do administrador de seu valor padrão. Esse controle falhará se o nome de usuário do administrador de um cluster do Redshift estiver definido como `awsuser`

Ao criar um banco de dados do Amazon RDS, você deve alterar o nome de usuário do administrador padrão para um valor exclusivo. Os nomes de usuário padrão são de conhecimento público e devem ser alterados na configuração. Alterar os nomes de usuário padrão reduz o risco de acesso não intencional.

Correção

Não é possível alterar o número da porta do cluster do Amazon Redshift depois que ela é criada. Para criar um cluster de banco de dados, siga as instruções em .

[Redshift.9] Os clusters do Redshift não devem usar o nome do banco de dados padrão

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Configuração de recursos

Severidade: média

Tipo de recurso

Regra do AWS Config : `redshift-default-db-name-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um cluster de banco de dados do Amazon RDS alterou o nome de usuário do administrador de seu valor padrão. Esse controle falhará se o nome de usuário do administrador de um cluster do Redshift estiver definido como `dev`

Ao criar um banco de dados do Amazon RDS, você deve alterar o nome de usuário do administrador padrão para um valor exclusivo. Os nomes de usuário padrão são de conhecimento público e devem ser alterados na configuração. Por exemplo, um nome conhecido poderia levar a um acesso inadvertido se fosse usado nas condições da política do IAM.

Correção

Não é possível alterar o número da porta do cluster do Amazon Redshift depois que ela é criada. Para obter instruções, consulte Conceitos básicos do Amazon Redshift no Guia de conceitos básicos do Amazon Redshift.

[Redshift.10] Os clusters do Redshift devem ser criptografados em repouso

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra do AWS Config : `redshift-cluster-kms-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se os clusters do Amazon Redshift estão criptografados em repouso. O controle falhará se um cluster do Redshift não for criptografado em repouso ou se a chave de criptografia for diferente da chave fornecida no parâmetro da regra.

No Amazon Redshift, é possível ativar a criptografia de banco de dados para seus clusters para ajudar a proteger os dados em repouso. Quando você ativar a criptografia de um cluster, os blocos de dados e os metadados do sistema serão criptografados para o cluster e os respectivos snapshots. A criptografia de dados em repouso é uma prática recomendada para adicionar uma camada de gerenciamento de acesso aos seus dados. Criptografar dados em repouso reduz o risco de um usuário não autenticado ter acesso aos dados armazenados em disco.

Correção

Para modificar um cluster do Redshift para usar a criptografia KMS, consulte Alterar criptografia do cluster no Guia de gerenciamento do Amazon Redshift.

[Redshift.11] Os clusters do Redshift devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-redshift-cluster` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um cluster do Amazon Redshift tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o cluster não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o cluster não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um cluster do Redshift, consulte Como marcar recursos no Amazon Redshift no Guia de gerenciamento do Amazon Redshift.

[Redshift.12] As assinaturas de notificação de eventos do Redshift devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-redshift-eventsubscription` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um snapshot de cluster do Amazon Redshift tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o snapshot do cluster não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle verificará apenas a existência de uma chave de tag e falhará se o instantâneo do cluster não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma assinatura de notificação de eventos do Redshift, consulte Como marcar recursos no Amazon Redshift no Guia de gerenciamento do Amazon Redshift.

[Redshift.13] Os instantâneos do cluster do Redshift devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-redshift-clustersnapshot` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um snapshot de cluster do Amazon Redshift tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o snapshot do cluster não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle verificará apenas a existência de uma chave de tag e falhará se o instantâneo do cluster não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM.

Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um snapshot de cluster do Redshift, consulte Como marcar recursos no Amazon Redshift no Guia de gerenciamento do Amazon Redshift.

[Redshift.14] Os grupos de sub-redes do cluster Redshift devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-redshift-clustersubnetgroup` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o	StringList	Lista de tags que atendem	`No default value`

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.		aos AWS requisitos	

Esse controle verifica se um grupo de sub-redes do cluster Amazon Redshift tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o grupo de sub-redes do cluster não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o grupo de sub-redes do cluster não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um grupo de sub-redes do cluster do Redshift, consulte Como marcar recursos no Amazon Redshift no Guia de gerenciamento do Amazon Redshift.

[Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas

Categoria: Proteger > Configuração de rede segura > Configuração do grupo de segurança

Severidade: alta

Tipo de recurso

Regra do AWS Config : `redshift-unrestricted-port-access`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um grupo de segurança associado a um cluster do Amazon Redshift tem regras de entrada que permitem acesso à porta do cluster pela Internet (0.0.0.0/0 ou: :/0). O controle falhará se as regras de entrada do grupo de segurança permitirem o acesso à porta do cluster pela Internet.

Permitir acesso de entrada irrestrito à porta de cluster do Redshift (endereço IP com sufixo /0) pode resultar em acesso não autorizado ou incidentes de segurança. Recomendamos aplicar o princípio de acesso com privilégios mínimos ao criar grupos de segurança e configurar regras de entrada.

Correção

Para restringir a entrada na porta do cluster Redshift a origens restritas, consulte Trabalhar com regras de grupos de segurança no Guia do usuário da Amazon VPC. Atualize regras em que o intervalo de portas corresponda à porta do cluster do Redshift e o intervalo de portas IP seja 0.0.0.0/0.

Conceitos do Amazon Route 53

Esses controles estão relacionados aos recursos da API de Gateway.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[Route53.1] As verificações de saúde do Route 53 devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

AWS Config regra: `tagged-route53-healthcheck` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se uma verificação de saúde do Amazon Route 53 tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a verificação de integridade não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle verificará apenas a existência de uma chave de tag e falhará se a verificação de integridade não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em

atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma verificação de saúde do Route 53, consulte Nomeação e marcação de verificações de saúde no Guia do desenvolvedor do Amazon Route 53.

As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `route53-query-logging-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o registro de consultas ao DNS está habilitado para uma zona hospedada pública do Amazon Route 53. Esse controle verifica se o registro de consultas ao DNS está habilitado para uma zona hospedada pública do Amazon Route 53.

O registro em log de consultas ao DNS para uma zona hospedada do Route 53 atende aos requisitos de segurança e conformidade do DNS e concede visibilidade. Os logs incluem informações como o domínio ou o subdomínio que foi consultado, a data e hora da consulta, o tipo de registro DNS (por exemplo, A ou AAAA) e o código de resposta do DNS (por exemplo, `NoError` ou `ServFail`). Quando o registro de consultas DNS está ativado, o Route 53 publica os arquivos de log no Amazon CloudWatch Logs.

Correção

Para registrar consultas ao DNS para zonas hospedadas públicas do Route 53, consulte Configurar registros em log para consultas ao DNS no Guia do desenvolvedor do Amazon Route 53.

Amazon Simple Storage Service Batch

Esses controles estão relacionados aos recursos da API de Gateway.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas

> **Important**
>
> Em 12 de março de 2024, o título desse controle foi alterado para o título mostrado. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.1.4, CIS Foundations Benchmark v1.4.0/2.1.5, PCI DSS v3.2.1/1.2.1, AWS PCI DSS v3.2.1/1.3.1, PCI DSS v3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, Nist.800-53.r5 AC-3, NiST.800-53.r5 AC-3 (7), Nist.800-53.r5 AC-4, NiST.800-53.r5 AC-4 (21), Nist.800-53.r5 AC-6, NiST.800-53.r5 SC-7 (11), Nist.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (21), NIST.800-53.R5 SC-7 (3), NIST.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-7 (9))

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso

Regra do AWS Config : `s3-account-level-public-access-blocks-periodic`

Tipo de programação: Periódico

Parâmetros:

- `ignorePublicAcls`: `true` (não personalizável)
- `blockPublicPolicy`: `true` (não personalizável)
- `blockPublicAcls`: `true` (não personalizável)
- `restrictPublicBuckets`: `true` (não personalizável)

Esse controle verifica se as configurações anteriores de acesso público do bloco Amazon S3 estão definidas no nível da conta para um bucket de uso geral do S3. O controle falhará se uma ou mais das configurações de acesso público do bloco estiverem definidas como`false`.

O controle falhará se alguma das configurações estiver definida como `false` ou se alguma das configurações não estiver definida.

O bloco de acesso público do Amazon S3 foi projetado para fornecer controles em um nível de bucket S3 inteiro Conta da AWS ou individual para garantir que os objetos nunca tenham acesso público. O acesso público aos buckets e objetos é concedido através de listas de controle de acesso (ACLs), políticas de bucket ou ambos.

A menos que você queira que os buckets do S3 sejam acessíveis publicamente, configure o recurso Acesso público de bloco do no nível da conta.

Para obter mais informações, consulte Usar o bloqueio de acesso público do Amazon S3 no Guia do desenvolvedor do Amazon Simple Storage Service.

Correção

Para habilitar o Amazon S3 para bloquear o acesso público para você Conta da AWS, consulte Definir configurações de bloqueio de acesso público para sua conta no Guia do usuário do Amazon Simple Storage Service.

[S3.2] Os buckets de uso geral do S3 devem bloquear o acesso público de leitura

> **Important**
>
> Em 12 de março de 2024, o título desse controle foi alterado para o título mostrado. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Requisitos relacionados: PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/1.3.2,PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

Categoria: Proteger > Configuração de rede segura

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `s3-bucket-public-read-prohibited`

Tipo de programação: periódico e acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um bucket de uso geral do Amazon S3 permite acesso público de leitura. Ele avalia as configurações de bloqueio de acesso público, a política do bucket e a lista de controle de acesso (ACL) do bucket. O controle falhará se o bucket permitir acesso público de leitura.

Alguns casos de uso exigem que todos na Internet possam ler a partir do bucket do S3. Entretanto, essas situações são raras. Para garantir a integridade e a segurança dos dados, o bucket do S3 não deve ser legível publicamente.

Correção

Para saber mais sobre as configurações de bloqueio de acesso público para buckets do S3, consulte Bloqueio do acesso público ao seu armazenamento no Amazon S3 no Guia do Usuário do Amazon Simple Storage Service.

[S3.3] Os buckets de uso geral do S3 devem bloquear o acesso público de gravação

> **Important**
>
> Em 12 de março de 2024, o título desse controle foi alterado para o título mostrado. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Requisitos relacionados: PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/1.3.2,PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

Categoria: Proteger > Configuração de rede segura

Severidade: crítica

Tipo de recurso

Regra do AWS Config : `s3-bucket-public-write-prohibited`

Tipo de programação: periódico e acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um bucket de uso geral do Amazon S3 permite acesso público de gravação. Ele avalia as configurações de bloqueio de acesso público, a política do bucket e a lista de controle de acesso (ACL) do bucket. O controle falhará se o bucket permitir acesso público de gravação.

Alguns casos de uso exigem que todos na Internet possam gravar no bucket do S3. Entretanto, essas situações são raras. Para garantir a integridade e a segurança dos dados, o bucket do S3 não deve ser gravável publicamente.

Correção

Para saber mais sobre as configurações de bloqueio de acesso público para buckets do S3, consulte Bloqueio do acesso público ao seu armazenamento no Amazon S3 no Guia do Usuário do Amazon Simple Storage Service.

[S3.5] Os buckets de uso geral do S3 devem exigir solicitações de uso de SSL

> **Important**
>
> Em 12 de março de 2024, o título desse controle foi alterado para o título mostrado. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.1.1, CIS Foundations Benchmark v1.4.0/2.1.2, PCI DSS v3.2.1/4.1, NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3) Nist.800-53.r5 SC-13, NIST.800-53.r5 SC-23, Nist.800-53.r5 SC-23 (3), Nist.800-53.R5 SC-7 (4), NIST.800-53.R5 SC-8, Nist.800-53.R5 SC-8 (1), Nist.800-53.R5 SC-8 (2), NIST.800-53.5R SI-7 (6) AWS

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `s3-bucket-ssl-requests-only`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um bucket de uso geral do Amazon S3 tem uma política que exige que as solicitações usem SSL. O controle falhará se a política do bucket não exigir que as solicitações usem SSL.

Os buckets do S3 devem ter políticas que exijam que todas as solicitações (`Action: S3:*`) aceitem somente a transmissão de dados por HTTPS na política de recursos do S3, indicada pela chave de condição `aws:SecureTransport`.

Correção

Para atualizar uma política de bucket do Amazon S3 para negar transporte não seguro, consulte Adicionar uma política de bucket usando o console do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Adicione uma declaração de política semelhante à da política a seguir. Substitua pelo nome do bucket criado em .

```
{
    "Id": "ExamplePolicy",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ],
            "Condition": {
                "Bool": {
                     "aws:SecureTransport": "false"
                }
            },
           "Principal": "*"
        }
    ]
}
```

Para obter mais informações, consulte Qual política de bucket do S3 devo usar para cumprir a AWS Config regra s3-? bucket-ssl-requests-only no Centro de Conhecimento AWS Oficial.

[S3.6] As políticas de bucket de uso geral do S3 devem restringir o acesso a outros Contas da AWS

> **Important**
>
> Em 12 de março de 2024, o título desse controle foi alterado para o título mostrado. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Proteger > Gerenciamento de acesso seguro > Ações confidenciais de API restritas

Severidade: alta

Tipo de recurso

Regra do AWS Config: `s3-bucket-blacklisted-actions-prohibited`

Tipo de programação: acionado por alterações

Parâmetros:

- `blacklistedactionpatterns`: `s3:DeleteBucketPolicy, s3:PutBucketAcl, s3:PutBucketPolicy, s3:PutEncryptionConfiguration, s3:PutObjectAcl` (não personalizável)

Esse controle verifica se uma política de bucket de uso geral do Amazon S3 impede que diretores de outras Contas da AWS pessoas executem ações negadas em recursos no bucket S3. O controle falhará se a política de bucket permitir uma ou mais das ações anteriores para um principal em outro Conta da AWS.

A implementação do privilégio de acesso mínimo é fundamental para reduzir o risco de segurança e o impacto que pode resultar de erros ou usuários mal-intencionados. Se uma política de bucket do S3 permitir o acesso de contas externas, isso poderá resultar na exfiltração de dados por uma ameaça interna ou por um invasor.

O parâmetro `blacklistedactionpatterns` permite uma avaliação bem-sucedida da regra para buckets do S3. O parâmetro concede acesso a contas externas para padrões de ação que não estão incluídos na lista `blacklistedactionpatterns`.

Correção

Para atualizar uma política de bucket do Amazon S3 para negar transporte não seguro, consulte Adicionar uma política de bucket usando o console do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Na página Editar política do bucket, na caixa de texto de edição da política, execute uma das seguintes ações:

- Remova as declarações que concedem a outras Contas da AWS acesso às ações negadas.
- Remova as ações negadas permitidas das declarações.

[S3.7] Os buckets de uso geral do S3 devem usar a replicação entre regiões

> **Important**
>
> Em 12 de março de 2024, o título desse controle foi alterado para o título mostrado. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: baixa

Tipo de recurso

AWS Config regra: **`s3-bucket-cross-region-replication-enabled`**

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um bucket de uso geral do Amazon S3 tem a replicação entre regiões ativada. O controle falhará se o bucket não tiver a replicação entre regiões ativada.

A replicação é a cópia automática e assíncrona de objetos entre buckets iguais ou diferentes. Regiões da AWS A replicação copia os objetos recém-criados e as atualizações de objeto de um bucket de origem para um bucket de destino. As melhores práticas da AWS recomendam a replicação para os buckets de origem e destino que são propriedade da mesma Conta da AWS. Além da disponibilidade, você deve considerar outras configurações de proteção de sistemas.

Correção

Para habilitar a replicação entre regiões em um bucket do S3, consulte Configurar a replicação para buckets de origem e destino pertencentes à mesma conta no Guia do usuário do Amazon Simple Storage Service. Em Source bucket, escolha Aplicar a todos os objetos no bucket.

[S3.8] Os buckets de uso geral do S3 devem bloquear o acesso público

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.1.4, AWS CIS Foundations Benchmark v1.4.0/2.1.5, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-4 (21) Nist.800-53.R5 AC-6, Nist.800-53.R5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.R5 SC-7 (16), NIST.800-53.R5 SC-7 (20), NIST.800-53.R5 SC-7 (3)), Nist.800-53.r5 SC-7 (4), Nist.800-53.r5 SC-7 (9)

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: alta

Tipo de recurso

Regra do AWS Config : `s3-bucket-level-public-access-prohibited`

Tipo de programação: acionado por alterações

Parâmetros:

- `excludedPublicBuckets` (não personalizável): uma lista separada por vírgulas de nomes de buckets do S3 públicos permitidos conhecidos

Esse controle verifica se um bucket de uso geral do Amazon S3 bloqueia o acesso público no nível do bucket. O controle falhará se alguma das seguintes configurações for definida como`false`:

- `ignorePublicAcls`
- `blockPublicPolicy`
- `blockPublicAcls`
- `restrictPublicBuckets`

O bloco de acesso público do foi projetado para fornecer controles para toda a conta da ou no nível do bucket do S3 individual para garantir que os objetos nunca tenham acesso público. O acesso público aos buckets e objetos é concedido através de listas de controle de acesso (ACLs), políticas de bucket ou ambos.

A menos que você queira que os buckets do S3 sejam acessíveis publicamente, configure o recurso Acesso público de bloco do no nível da conta.

Correção

Para obter informações sobre como remover o acesso público em um nível de bucket, consulte Bloquear o acesso público ao seu armazenamento do Amazon S3 no Guia do usuário do Amazon S3.

[S3.9] Os buckets de uso geral do S3 devem ter o registro de acesso ao servidor ativado

> **Important**
>
> Em 12 de março de 2024, o título desse controle foi alterado para o título mostrado. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `s3-bucket-logging-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o registro de acesso ao servidor está habilitado para um bucket de uso geral do Amazon S3. O controle falhará se o registro de acesso ao servidor não estiver ativado. Quando você habilita o registro em log, o Amazon S3 entrega logs de acesso a um bucket de origem ou de destino de sua escolha. O bucket de destino deve estar no Região da AWS mesmo bucket de origem e não deve ter um período de retenção padrão configurado. O bucket de registro em log de destino não precisa ter o registro em log de acesso ao servidor ativado, e você deve suprimir as descobertas desse bucket.

O registro em log de acesso ao servidor fornece detalhes sobre as solicitações que são feitas a um bucket. Os logs de acesso ao servidor podem auxiliar nas auditorias de segurança e acesso. Para

obter mais informações, consulte Melhores práticas de segurança para o Amazon S3: Habilitar o registro em log de acesso ao servidor do Amazon S3.

Correção

Para habilitar o registro de acesso ao servidor para seu bucket do CloudTrail S3, consulte Habilitar registro em log de acesso ao servidor do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

[S3.10] Os buckets de uso geral do S3 com controle de versão ativado devem ter configurações de ciclo de vida

> **Important**
>
> Em 12 de março de 2024, o título desse controle foi alterado para o título mostrado. O Security Hub retirou esse controle em abril de 2024 do padrão AWS Foundational Security Best Practices, mas ele ainda está incluído no padrão NIST SP 800-53 Rev. 5. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `s3-version-lifecycle-policy-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um bucket versionado de uso geral do Amazon S3 tem uma configuração de ciclo de vida. O controle falhará se o bucket não tiver uma configuração de ciclo de vida.

Recomendamos criar uma configuração de ciclo de vida para seu bucket do S3 para ajudá-lo a definir as ações que você deseja que o Amazon S3 execute durante a vida útil de um objeto.

Correção

Para obter mais informações sobre como configurar o ciclo de vida em um bucket do Amazon S3, consulte Definir a configuração do ciclo de vida em um bucket e Gerenciar seu ciclo de vida de armazenamento.

[S3.11] Os buckets de uso geral do S3 devem ter as notificações de eventos ativadas

> **Important**
>
> Em 12 de março de 2024, o título desse controle foi alterado para o título mostrado. O Security Hub retirou esse controle em abril de 2024 do padrão AWS Foundational Security Best Practices, mas ele ainda está incluído no padrão NIST SP 800-53 Rev. 5:. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `s3-event-notifications-enabled`

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`eventTypes`	Lista de tipos de eventos do S3 preferidos	EnumList (máximo de 28 itens)	`s3:IntelligentTiering`, `s3:Lifecy`	Nenhum valor padrão

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
			cleExpiration:*, s3:LifecycleExpiration:Delete, s3:LifecycleExpiration:DeleteMarkerCreated, s3:LifecycleTransition, s3:ObjectAcl:Put, s3:ObjectCreated:*, s3:ObjectCreated:CompleteMultipartUpload, s3:ObjectCreated:Copy, s3:ObjectCreated:Post, s3:ObjectCreated:P	

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
			ut, s3:ObjectRemoved:*, s3:ObjectRemoved:Delete, s3:ObjectRemoved:DeleteMarkerCreated, s3:ObjectRestore:*, s3:ObjectRestore:Completed, s3:ObjectRestore:Delete, s3:ObjectRestore:Post, s3:ObjectTagging:*, s3:ObjectTagging:Delete, s3:ObjectTagging:P	

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
			ut, s3:ReducedRedundancyLostObject, s3:Replication:*, s3:Replication:OperationFailedReplication, s3:Replication:OperationMissedThreshold, s3:Replication:OperationNotTracked, s3:Replication:OperationReplicatedAfterThreshold, s3:TestEvent	

Esse controle verifica se as notificações de eventos do S3 estão habilitadas em um bucket de uso geral do Amazon S3. O controle falhará se as notificações de eventos do S3 não estiverem habilitadas no bucket. Se você fornecer valores personalizados para o `eventTypes` parâmetro, o controle será aprovado somente se as notificações de eventos estiverem habilitadas para os tipos de eventos especificados.

Ao ativar as notificações de eventos do S3, você recebe alertas quando ocorrem eventos específicos que afetam seus buckets do S3. Por exemplo, é possível ser notificado sobre a criação, remoção e restauração de objetos. Essas notificações podem alertar as equipes relevantes sobre modificações acidentais ou intencionais que podem levar ao acesso não autorizado aos dados.

Correção

Para obter informações sobre a detecção de alterações em buckets e objetos do S3, consulte Notificações de eventos do Amazon S3 no Guia do usuário do Amazon S3.

[S3.12] As ACLs não devem ser usadas para gerenciar o acesso do usuário aos buckets de uso geral do S3

> **Important**
>
> Em 12 de março de 2024, o título desse controle foi alterado para o título mostrado. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Requisitos relacionados: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(15), NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-6

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `s3-bucket-acl-prohibited`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um bucket de uso geral do Amazon S3 fornece permissões de usuário com uma lista de controle de acesso (ACL). O controle falhará se uma ACL estiver configurada para gerenciar o acesso do usuário no bucket.

As ACLs são mecanismos de controle de acesso que antecedem o IAM. Em vez de ACLs, recomendamos usar políticas de bucket do S3 ou políticas AWS Identity and Access Management (IAM) para gerenciar o acesso aos seus buckets do S3.

Correção

Para passar esse controle, você deve desativar as ACLs para seus buckets do S3. Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs para seu bucket, no Guia do Usuário do Amazon S3.

Para criar uma política de bucket do S3, consulte Adicionar uma política de bucket usando o console do Amazon S3. Para criar uma política de usuário do IAM em um bucket do S3, consulte Controle do acesso a um bucket com políticas de usuário.

[S3.13] Os buckets de uso geral do S3 devem ter configurações de ciclo de vida

> **Important**
>
> Em 12 de março de 2024, o título desse controle foi alterado para o título mostrado. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

Categoria: Proteger > Proteção de dados

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `s3-lifecycle-policy-check`

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`targetTransitionDays`	Número de dias após a criação do objeto em que os objetos farão a transição para a classe de armazenamento especificada.	Inteiro	1 para 36500	Nenhum valor padrão
`targetExpirationDays`	Número de dias após a criação do objeto quando os objetos são excluídos.	Inteiro	1 para 36500	Nenhum valor padrão
`targetTransitionStorageClass`	Tipo de classe de armazenamento do S3 de destino	Enum	`STANDARD_IA`, `INTELLIGENT_TIERING`, `ONEZONE_IA`, `GLACIER`, `GLACIER_IR`, `DEEP_ARCHIVE`	Nenhum valor padrão

Esse controle verifica se um bucket de uso geral do Amazon S3 tem uma configuração de ciclo de vida. O controle falhará se o bucket não tiver uma configuração de ciclo de vida. Se você fornecer valores personalizados para um ou mais dos parâmetros anteriores, o controle será aprovado somente se a política incluir a classe de armazenamento, o tempo de exclusão ou o tempo de transição especificados.

A criação de uma configuração de ciclo de vida para seu bucket do S3 define as ações que você deseja que o Amazon S3 execute durante a vida útil de um objeto. Por exemplo, é possível criar

uma política de ciclo de vida que fará a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado.

Correção

Para obter mais informações sobre como configurar o ciclo de vida em um bucket do Amazon S3, consulte Definir a configuração do ciclo de vida em um bucket e Gerenciar seu ciclo de vida de armazenamento.

[S3.14] Os buckets de uso geral do S3 devem ter o controle de versão ativado

> **Important**
>
> Em 12 de março de 2024, o título desse controle foi alterado para o título mostrado. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Categoria: Proteger > Proteção de dados > Proteção contra exclusão de dados

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Severidade: baixa

Tipo de recurso

Regra do AWS Config : `s3-bucket-versioning-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um bucket de uso geral do Amazon S3 tem o versionamento ativado. O controle falhará se o controle de versão do bucket for suspenso.

Use o versionamento do S3 para manter diversas variantes de um objeto no mesmo bucket. O versionamento pode ser usado para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do . O versionamento do S3 ajuda você a se recuperar de ações não intencionais de usuários e de falhas da aplicação.

> **Tip**
>
> À medida que o número de objetos aumenta em um bucket devido ao controle de versão, você pode definir uma configuração de ciclo de vida para arquivar ou excluir automaticamente objetos versionados com base em regras. Para obter mais informações, consulte o Gerenciamento do ciclo de vida do objeto no Guia do usuário do Amazon S3.

Correção

Para usar o controle de versão em um bucket do S3, consulte Habilitar o versionamento em buckets no Guia do usuário do Amazon S3.

[S3.15] Os buckets de uso geral do S3 devem ter o Object Lock ativado

> **Important**
>
> Em 12 de março de 2024, o título desse controle foi alterado para o título mostrado. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Categoria: Proteger > Proteção de dados > Proteção contra exclusão de dados

Requisitos relacionados: NIST.800-53.r5 CA-7

Severidade: média

Tipo de recurso

AWS Config regra: **`s3-bucket-default-lock-enabled`**

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`mode`	Modo de retenção do Bloqueio de objetos do S3	Enum	`GOVERNANCE`, `COMPLIANCE`	Nenhum valor padrão

Esse controle verifica se um bucket de uso geral do Amazon S3 tem o Object Lock ativado. O controle falhará se o Object Lock não estiver habilitado para o bucket. Se você fornecer um valor personalizado para o parâmetro `mode`, o controle passará somente se o Bloqueio de objetos do S3 usar o modo de retenção especificado.

Você pode usar o S3 Object Lock para armazenar objetos usando um modelo write-once-read-many (WORM). O bloqueio de objetos pode ajudar a evitar que os objetos sejam excluídos ou substituídos por um período de tempo fixo ou indefinidamente. É possível usar o bloqueio de objetos do S3 para atender a requisitos regulamentares que exigem armazenamento WORM ou adicionar uma camada extra de proteção contra alterações e exclusões de objetos.

Correção

Para configurar o Bloqueio de objetos para buckets do S3 novos e existentes, consulte Configuração do Bloqueio de objetos do S3 no Guia do usuário do Amazon S3.

[S3.17] Os buckets de uso geral do S3 devem ser criptografados em repouso com AWS KMS keys

> **Important**
>
> Em 12 de março de 2024, o título desse controle foi alterado para o título mostrado. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Severidade: média

Tipo de recurso

AWS Config regra: **`s3-default-encryption-kms`**

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um bucket de uso geral do Amazon S3 está criptografado com um AWS KMS key (SSE-KMS ou DSSE-KMS). O controle falhará se o bucket for criptografado com criptografia padrão (SSE-S3).

A criptografia do lado do servidor é a criptografia de dados em seu destino pela aplicação ou serviço que os recebe. A menos que você especifique o contrário, os buckets do S3 usam as chaves gerenciadas pelo Amazon S3 (SSE-S3) por padrão para a criptografia do lado do servidor. No entanto, para maior controle, você pode optar por configurar buckets para usar criptografia do lado do servidor (SSE-KMS ou DSSE-KMS AWS KMS keys) em vez disso. O Amazon S3 criptografa seus dados no nível do objeto à medida que os grava em discos em AWS datacenters e os descriptografa para você quando você os acessa.

Correção

Para criptografar um bucket do S3 usando o SSE-KMS, consulte Especificação da criptografia do lado do servidor com (SSE-KMS) no Guia do usuário do Amazon AWS KMS S3. Para criptografar um bucket do S3 usando o DSSE-KMS, consulte Especificação da criptografia de duas camadas no lado do servidor com (AWS KMS keys DSSE-KMS) no Guia do usuário do Amazon S3.

[S3.19] Os pontos de acesso do S3 devem ter configurações de bloqueio do acesso público habilitadas

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Gerenciamento de acesso seguro > Recursos não acessíveis ao público

Severidade: crítica

Tipo de recurso

AWS Config regra: **s3-access-point-public-access-blocks**

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um ponto de acesso Amazon S3 tem configurações de bloqueio de acesso público habilitadas. O controle falhará se as configurações de bloqueio de acesso público não estiverem habilitadas para o ponto de acesso.

O recurso Bloqueio de acesso público do Amazon S3 ajuda você a gerenciar o acesso aos recursos do S3 em três níveis: conta, bucket e ponto de acesso. As configurações em cada nível podem ser definidas de forma independente, permitindo que você tenha diferentes níveis de restrições de acesso público aos seus dados. As configurações do ponto de acesso não podem substituir individualmente as configurações mais restritivas em níveis mais altos (nível da conta ou bucket atribuído ao ponto de acesso). Em vez disso, as configurações no nível do ponto de acesso são aditivas, o que significa que elas complementam e funcionam junto com as configurações nos outros níveis. A menos que você pretenda que um ponto de acesso do S3 seja publicamente acessível, você deverá habilitar as configurações de bloqueio de acesso público.

Correção

Atualmente, o Amazon S3 não oferece suporte à alteração das configurações do bloqueio de acesso público após à criação de um ponto de acesso. Todas as configurações do bloqueio de acesso público são habilitadas por padrão quando você cria um novo pontos de acesso. Recomendamos que você mantenha todas as configurações ativadas, a menos que saiba que tem uma necessidade específica de desativar qualquer uma delas. Para obter mais informações, consulte Gerenciamento do acesso público a pontos de acesso no Guia do usuário do Amazon Simple Storage Service.

[S3.20] Os buckets de uso geral do S3 devem ter a exclusão de MFA habilitada

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/2.1.2, CIS Foundations Benchmark v1.4.0/2.1.3, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 AWS CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoria: Proteger > Proteção de dados > Proteção contra exclusão de dados

Severidade: baixa

Tipo de recurso

AWS Config regra: **s3-bucket-mfa-delete-enabled**

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se a exclusão da autenticação multifator (MFA) está habilitada em um bucket versionado de uso geral do Amazon S3. O controle falhará se a exclusão de MFA não estiver habilitada no bucket. O controle não produz descobertas para buckets que têm uma configuração de ciclo de vida.

Ao trabalhar com o versionamento do S3 em buckets do Amazon S3, é possível, opcionalmente, adicionar outra camada de segurança configurando um bucket para habilitar a exclusão de MFA. Quando você faz isso, o proprietário do bucket precisa incluir dois formulários de autenticação em qualquer solicitação para excluir uma versão ou modificar o estado de versionamento do bucket. A exclusão de MFA fornece segurança adicional caso suas credenciais de segurança sejam comprometidas. A exclusão de MFA também pode ajudar a evitar exclusões acidentais de buckets exigindo que o usuário que inicia a ação de exclusão para provar a posse física de um dispositivo de MFA com um código de MFA e adicionando uma camada extra de atrito e segurança à ação de exclusão.

> **Note**
>
> O recurso de exclusão de MFA exige versionamento do bucket como uma dependência. O versionamento de buckets é um meio de manter diversas variantes de um objeto do S3 no mesmo bucket. Além disso, somente o proprietário do bucket que está conectado como usuário raiz pode habilitar a exclusão do MFA e realizar ações de exclusão nos buckets do S3.

Correção

Para habilitar o versionamento do S3 e configurar a exclusão de MFA em um bucket, consulte Configuração da exclusão de MFA no Guia do usuário do Amazon Simple Storage Service.

[S3.22] Os buckets de uso geral do S3 devem registrar eventos de gravação em nível de objeto

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/3.8

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

AWS Config regra: **`cloudtrail-all-write-s3-data-event-check`**

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se há pelo menos uma Conta da AWS trilha AWS CloudTrail multirregional que registra todos os eventos de dados de gravação para buckets do Amazon S3. O controle falhará se a conta não tiver uma trilha multirregional que registre eventos de dados de gravação para buckets do S3.

As operações em nível de objeto do S3, como`GetObject`, e `DeleteObject``PutObject`, são chamadas de eventos de dados. Por padrão, CloudTrail não registra eventos de dados, mas você pode configurar trilhas para registrar eventos de dados para buckets do S3. Ao ativar o registro em nível de objeto para eventos de gravação de dados, você pode registrar o acesso de cada objeto (arquivo) individual em um bucket do S3. Habilitar o registro em nível de objeto pode ajudá-lo a atender aos requisitos de conformidade de dados, realizar análises de segurança abrangentes, monitorar padrões específicos de comportamento do usuário e agir sobre a atividade de API em nível de objeto em seus buckets do S3 usando o Amazon Events. Conta da AWS CloudWatch Esse controle produz uma `PASSED` descoberta se você configurar uma trilha multirregional que registra somente gravação ou todos os tipos de eventos de dados para todos os buckets do S3.

Correção

Para habilitar o registro em nível de objeto para buckets do S3, consulte Ativação do registro de CloudTrail eventos para buckets e objetos do S3 no Guia do usuário do Amazon Simple Storage Service.

[S3.23] Os buckets de uso geral do S3 devem registrar eventos de leitura em nível de objeto

Requisitos relacionados: CIS AWS Foundations Benchmark v3.0.0/3.9

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

AWS Config regra: **`cloudtrail-all-read-s3-data-event-check`**

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se há pelo menos uma Conta da AWS trilha AWS CloudTrail multirregional que registra todos os eventos de dados lidos dos buckets do Amazon S3. O controle falhará se a conta não tiver uma trilha multirregional que registre eventos de dados de leitura para buckets do S3.

As operações em nível de objeto do S3, como`GetObject`, e `DeleteObject``PutObject`, são chamadas de eventos de dados. Por padrão, CloudTrail não registra eventos de dados, mas você pode configurar trilhas para registrar eventos de dados para buckets do S3. Ao habilitar o registro em nível de objeto para eventos de leitura de dados, você pode registrar o acesso de cada objeto (arquivo) individual em um bucket do S3. Habilitar o registro em nível de objeto pode ajudá-lo a atender aos requisitos de conformidade de dados, realizar análises de segurança abrangentes, monitorar padrões específicos de comportamento do usuário e agir sobre a atividade de API em nível de objeto em seus buckets do S3 usando o Amazon Events. Conta da AWS CloudWatch Esse controle produz uma `PASSED` descoberta se você configurar uma trilha multirregional que registra somente leitura ou todos os tipos de eventos de dados para todos os buckets do S3.

Correção

Para habilitar o registro em nível de objeto para buckets do S3, consulte Ativação do registro de CloudTrail eventos para buckets e objetos do S3 no Guia do usuário do Amazon Simple Storage Service.

SageMaker Controles da Amazon

Esses controles estão relacionados aos SageMaker recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet

Requisitos relacionados: PCI DSS v3.2.1/1.2.1,PCI DSS v3.2.1/1.3.1,PCI DSS v3.2.1/1.3.4,PCI DSS v3.2.1/1.3.2,PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3(7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4(21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), NIST.800-53.r5 SC-7(20), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-7(9)

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso

Regra do AWS Config : `sagemaker-notebook-no-direct-internet-access`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o acesso direto à Internet está desativado para uma instância de SageMaker notebook. O controle falhará se o `DirectInternetAccess` campo estiver habilitado para a instância do notebook.

Se você configurar sua SageMaker instância sem uma VPC, por padrão, o acesso direto à Internet será habilitado em sua instância. Você deve configurar sua instância com uma VPC e alterar a configuração padrão para Desabilitar — acessar a internet por meio de uma VPC. Para treinar ou hospedar modelos a partir de um notebook, você precisa de acesso à internet. Para habilitar o acesso à Internet, sua VPC deve ter um endpoint de interface (AWS PrivateLink) ou um gateway NAT e um grupo de segurança que permita conexões de saída. Para saber mais sobre como conectar uma instância de notebook a recursos em uma VPC, consulte Conectar uma instância de notebook a recursos em uma VPC no Amazon Developer Guide. SageMaker Você também deve garantir que o acesso à sua SageMaker configuração seja limitado somente aos usuários autorizados. Restrinja as permissões do IAM que permitem que os usuários alterem SageMaker configurações e recursos.

Correção

Você não pode alterar a configuração do acesso à internet depois de criar uma instância do notebook. Em vez disso, é possível parar, excluir e recriar a instância com acesso bloqueado à internet. Para excluir uma instância de notebook que permite acesso direto à Internet, consulte Usar instâncias de notebook para criar modelos: Limpeza no Amazon SageMaker Developer Guide. Para recriar uma instância do notebook que nega o acesso à internet, consulte Criar uma instância do notebook. Em Rede, Acesso direto à internet, escolha Desabilitar — Acessar a internet por meio de uma VPC.

[SageMaker.2] as instâncias do SageMaker notebook devem ser iniciadas em uma VPC personalizada

Requisitos relacionados: NIST.800-53.r5 AC-17(2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5(1), NIST.800-53.r5 SC-12(3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23(3), NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8(1), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Configuração de rede segura

Severidade: alta

Tipo de recurso

Regra do AWS Config : `sagemaker-notebook-instance-inside-vpc`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma instância de SageMaker notebook da Amazon é iniciada em uma nuvem privada virtual (VPC) personalizada. Esse controle falhará se uma instância do SageMaker notebook não for iniciada em uma VPC personalizada ou se for iniciada na SageMaker VPC de serviço.

Uma sub-rede é um intervalo de endereços IP em uma VPC. Recomendamos manter seus recursos dentro de uma VPC personalizada sempre que possível para garantir a proteção segura da rede de sua infraestrutura. Uma Amazon VPC é uma rede virtual dedicada à sua. Conta da AWS Com uma Amazon VPC, você pode controlar o acesso à rede e a conectividade com a Internet das instâncias do SageMaker Studio e do notebook.

Correção

Você não pode alterar a configuração do acesso à internet depois de criar uma instância do notebook. Em vez disso, é possível parar, excluir e recriar a instância com acesso bloqueado à internet. Para obter instruções, consulte Usar instâncias de notebook para criar modelos: Limpeza no Amazon SageMaker Developer Guide.

[SageMaker.3] Os usuários não devem ter acesso root às instâncias do SageMaker notebook

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Gerenciamento de acesso seguro > Recursos não acessíveis ao público

Severidade: alta

Tipo de recurso

Regra do AWS Config : `sagemaker-notebook-instance-root-access-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o acesso root está ativado para uma instância de SageMaker notebook da Amazon. O controle falhará se o acesso root estiver ativado para uma instância do SageMaker notebook.

Seguindo o princípio do privilégio mínimo, é uma prática recomendada de segurança restringir o acesso raiz aos recursos da instância para evitar o provisionamento excessivo involuntário de permissões.

Correção

Para restringir o acesso root às instâncias do SageMaker notebook, consulte Controlar o acesso root a uma instância do SageMaker notebook no Amazon SageMaker Developer Guide.

[SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1

Requisitos relacionados: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-36, Nist.800-53.r5 SA-13

Categoria: Recuperação > Resiliência > Alta disponibilidade

Severidade: média

Tipo de recurso

Regra do AWS Config : `sagemaker-endpoint-config-prod-instance-count`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se as variantes de produção de um SageMaker endpoint da Amazon têm uma contagem inicial de instâncias maior que 1. O controle falhará se as variantes de produção do endpoint tiverem apenas 1 instância inicial.

Variantes de produção executadas com uma contagem de instâncias maior que 1 permitem a redundância de instâncias Multi-AZ gerenciada por. SageMaker A implantação de recursos em várias zonas de disponibilidade é uma prática AWS recomendada para fornecer alta disponibilidade em sua arquitetura. A alta disponibilidade ajuda você a se recuperar de incidentes de segurança.

> **Note**
>
> Esse controle se aplica somente à configuração de endpoint baseada em instância.

Correção

Para obter mais informações sobre os parâmetros da configuração do endpoint, consulte Criar uma configuração de endpoint no Amazon SageMaker Developer Guide.

AWS Secrets Manager controles

Esses controles estão relacionados aos recursos do CloudFormation.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[SecretsManager.1] Os segredos do Secrets Manager devem ter a rotação automática ativada

Requisitos relacionados: NIST.800-53.r5 SC-28 (3), NIST.800-53.r5 SC-7 (16)

Categoria: Proteger > Desenvolvimento seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `secretsmanager-rotation-enabled-check`

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`maximumAllowedRotationFrequency`	Número máximo de dias permitidos para a frequência de rotação do segredo	Inteiro	`1` para `365`	Nenhum valor padrão

Esse controle verifica se um segredo armazenado AWS Secrets Manager está configurado com rotação automática. O controle falhará se o segredo não estiver configurado com rotação automática. Se você fornecer um valor personalizado para o parâmetro `maximumAllowedRotationFrequency`, o controle passará somente se o segredo for rotacionado automaticamente dentro da janela de tempo especificada.

O Secrets Manager ajuda você a melhorar a postura de segurança de sua organização. Os segredos podem ser credenciais de banco de dados, senhas, chaves de API de terceiros e até mesmo texto arbitrário. É possível usar o Secrets Manager para armazenar segredos centralmente, criptografar segredos automaticamente, controlar o acesso aos segredos e alternar segredos de forma segura e automática.

O Secrets Manager pode alternar segredos. É possível usar a alternância para substituir segredos de longo prazo por segredos de curto prazo. A alternância de seus segredos limita por quanto tempo um usuário não autorizado pode usar um segredo comprometido. Por esse motivo, você deve alternar seus segredos com frequência. Para saber mais sobre rotação, consulte Como girar seus AWS Secrets Manager segredos no Guia do AWS Secrets Manager usuário.

Correção

Para ativar a rotação automática dos segredos do Secrets Manager, consulte Configurar a rotação automática para AWS Secrets Manager segredos usando o console no Guia AWS Secrets Manager do Usuário. Você deve escolher e configurar uma AWS Lambda função para rotação.

[SecretsManager.2] Os segredos do Secrets Manager configurados com rotação automática devem girar com sucesso

Requisitos relacionados: NIST.800-53.r5 SC-28 (3), NIST.800-53.r5 SC-7 (16)

Categoria: Proteger > Desenvolvimento seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `secretsmanager-scheduled-rotation-success-check`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um AWS Secrets Manager segredo foi rotacionado com sucesso com base no cronograma de rotação. O controle falha se `RotationOccurringAsScheduled` estiver definido como `false`. O controle avalia apenas segredos que têm a alternância ativada.

O Secrets Manager ajuda você a melhorar a postura de segurança de sua organização. Os segredos podem ser credenciais de banco de dados, senhas, chaves de API de terceiros e até mesmo texto arbitrário. É possível usar o Secrets Manager para armazenar segredos centralmente, criptografar segredos automaticamente, controlar o acesso aos segredos e alternar segredos de forma segura e automática.

O Secrets Manager pode alternar segredos. É possível usar a alternância para substituir segredos de longo prazo por segredos de curto prazo. A alternância de seus segredos limita por quanto tempo um usuário não autorizado pode usar um segredo comprometido. Por esse motivo, você deve alternar seus segredos com frequência.

Além de configurar segredos para alternar automaticamente, você deve garantir que esses segredos sejam alternados com sucesso com base na programação de alternância.

Para saber mais sobre alternância, consulte Alternar seus segredos do AWS Secrets Manager no Guia do usuário do AWS Secrets Manager .

Correção

Se a alternância automática falhar, o Secrets Manager pode ter encontrado erros na configuração. Para alternar segredos no , é necessário usar uma função Lambda que defina como interagir com o banco de dados ou com o serviço que tem o segredo.

Para obter ajuda para diagnosticar e corrigir erros comuns relacionados à rotação de segredos, consulte Solução de problemas de AWS Secrets Manager rotação de segredos no Guia do AWS Secrets Manager usuário.

[SecretsManager.3] Remover segredos não utilizados do Secrets Manager

Requisitos relacionados: NIST.800-53.r5 SC-28 (3), NIST.800-53.r5 SC-7 (16)

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `secretsmanager-secret-unused`

Tipo de programação: Periódico

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`unusedForDays`	Número máximo de dias em que um segredo pode permanecer sem uso	Inteiro	1 para 365	90

Esse controle verifica se um AWS Secrets Manager segredo foi acessado dentro do período de tempo especificado. O controle falhará se um segredo não for usado além do período de tempo

especificado. A menos que você forneça um valor de parâmetro personalizado para o período de acesso, o Security Hub usará um valor padrão de 90 dias.

Excluir segredos não utilizados é tão importante quanto alternar segredos. Segredos não utilizados podem ser abusados por seus antigos usuários, que não precisam mais acessar esses segredos. Além disso, à medida que mais usuários obtêm acesso a um segredo, alguém pode tê-lo manipulado incorretamente e vazado para uma entidade não autorizada, o que aumenta o risco de abuso. A exclusão de segredos não utilizados ajuda a revogar o acesso a segredos por usuários que não precisam mais deles. Ele também ajuda a reduzir o custo do uso do Secrets Manager. Portanto, é essencial excluir rotineiramente segredos não utilizados.

Correção

Para excluir segredos inativos do Secrets Manager, consulte Excluir um AWS Secrets Manager segredo no Guia do AWS Secrets Manager usuário.

[SecretsManager.4] Os segredos do Secrets Manager devem ser alternados dentro de um determinado número de dias

Requisitos relacionados: NIST.800-53.r5 SC-28 (3), NIST.800-53.r5 SC-7 (16)

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: média

Tipo de recurso

Regra do AWS Config : `secretsmanager-secret-periodic-rotation`

Tipo de programação: Periódico

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`maxDaysSinceRotation`	Número máximo de dias em que um segredo pode permanecer sem alterações	Inteiro	1 para `180`	`90`

Esse controle verifica se um AWS Secrets Manager segredo é rotacionado pelo menos uma vez dentro do período de tempo especificado. O controle falhará se um segredo não tiver sido rotacionado com pelo menos essa frequência. A menos que você forneça um valor de parâmetro personalizado para o período de rotação, o Security Hub usará um valor padrão de 90 dias.

A alternância de segredos pode ajudá-lo a reduzir o risco de uso não autorizado de seus segredos na sua Conta da AWS. Os segredos podem ser credenciais de banco de dados, senhas, chaves de API de terceiros e até mesmo texto arbitrário. Se você não alterar o segredos por um longo período, eles se tornam mais propensos a ser comprometidos.

À medida que mais usuários obtêm acesso a um segredo, pode ser possível que alguém o tenha manipulado incorretamente e que ele tenha vazado para uma entidade não autorizada. Os segredos podem ser vazados por logs e dados de cache. Eles podem ser compartilhados para fins de depuração e não alterados nem revogados quando a depuração for concluída. Por todos esses motivos, os segredos devem ser mudados com frequência.

É possível configurar a alternância automática para segredos no AWS Secrets Manager. Isso permite que você substitua os segredos de longo prazo por outros de curto prazo, reduzindo significativamente o risco de comprometimento. Com o Secrets Manager, é possível configurar uma programação de alternância automática para seus segredos. Para ter mais informações, consulte Alternar os segredos do AWS Secrets Manager no Guia do usuário do AWS Secrets Manager .

Correção

Para ativar a rotação automática dos segredos do Secrets Manager, consulte Configurar a rotação automática para AWS Secrets Manager segredos usando o console no Guia AWS Secrets Manager do Usuário. Você deve escolher e configurar uma AWS Lambda função para rotação.

[SecretsManager.5] Os segredos do Secrets Manager devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-secretsmanager-secret` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um AWS Secrets Manager segredo tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o segredo não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o segredo não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS

Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um segredo do Secrets Manager, consulte AWS Secrets Manager Segredos de tags no Guia AWS Secrets Manager do usuário.

AWS Service Catalog controles

Esses controles estão relacionados aos recursos do Service Catalog.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS

Requisitos relacionados: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-4, Nist.800-53.r5 AC-6, Nist.800-53.r5 CM-8, Nist.800-53.r5 SC-7

Categoria: Proteger > Gerenciamento de acesso seguro

Severidade: alta

Tipo de recurso

Regra do AWS Config : `servicecatalog-shared-within-organization`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se AWS Service Catalog compartilha portfólios dentro de uma organização quando a integração com AWS Organizations está habilitada. O controle falha se os portfólios não forem compartilhados dentro de uma organização.

O compartilhamento de portfólio somente dentro do Organizations ajuda a garantir que um portfólio não seja compartilhado de forma incorreta Contas da AWS. Para compartilhar um portfólio do Service Catalog com uma conta em uma organização, o Security Hub recomenda usar `ORGANIZATION_MEMBER_ACCOUNT` em vez de`ACCOUNT`. Isso simplifica a administração

ao controlar o acesso concedido à conta em toda a organização. Se você tiver uma necessidade comercial de compartilhar os portfólios do Service Catalog com uma conta externa, poderá suprimir automaticamente as descobertas desse controle ou desativá-lo.

Correção

Para habilitar o compartilhamento de portfólio com Organizations, consulte Sharing with AWS Organizations no Service Catalog Administrator Guide

Controles do Amazon Simple Email Service

Esses controles estão relacionados aos recursos do Amazon SES.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[SES.1] As listas de contatos do SES devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config: `tagged-ses-contactlist` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se uma lista de contatos do Amazon SES tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a lista de contatos não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a lista de contatos não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para [que serve o ABAC](#)? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como [marcar seus AWS recursos](#) no. Referência geral da AWS

Correção

Para adicionar tags a uma lista de contatos do Amazon SES, consulte [TagResource](#)na Referência da API v2 do Amazon SES.

[SES.2] Os conjuntos de configuração do SES devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config: `tagged-ses-configurationset` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se um conjunto de configurações do Amazon SES tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o conjunto de configurações não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o conjunto de configurações não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um conjunto de configurações do Amazon SES, consulte TagResourcena Referência da API v2 do Amazon SES.

Amazon Simple Notification Service

Esses controles estão relacionados aos recursos da API de Gateway.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[SNS.1] Os tópicos do SNS devem ser criptografados em repouso usando AWS KMS

> **Important**
>
> O Security Hub retirou esse controle em abril de 2024 do padrão AWS Foundational Security Best Practices, mas ele ainda está incluído no padrão NIST SP 800-53 Rev. 5. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra do AWS Config : `sns-encrypted-kms`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um tópico do Amazon SNS está criptografado em repouso usando chaves gerenciadas em AWS Key Management Service ()AWS KMS. Os controles falharão se o tópico do SNS não usar uma chave KMS para criptografia do lado do servidor (SSE). Por padrão, o SNS armazena mensagens e arquivos usando criptografia de disco. Para passar esse controle, você deve optar por usar uma chave KMS para criptografia em vez disso. Isso adiciona uma camada adicional de segurança e fornece mais flexibilidade no controle de acesso.

Criptografar dados em repouso reduz o risco de os dados armazenados em disco serem acessados por um usuário não autenticado. AWS As permissões da API são necessárias para descriptografar os dados antes que eles possam ser lidos. Recomendamos criptografar tópicos do SNS com chaves KMS para uma camada adicional de segurança.

Correção

Para habilitar o SSE para um tópico do SNS, consulte Habilitando a criptografia do lado do servidor (SSE) para um tópico do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service. Antes de usar o SSE, você também deve configurar AWS KMS key políticas para permitir a criptografia de tópicos e criptografia e descriptografia de mensagens. Para obter mais informações, consulte Configuração de AWS KMS permissões no Guia do desenvolvedor do Amazon Simple Notification Service.

O registro do status de entrega deve ser ativado para mensagens de notificação enviadas para um tópico

> **Important**
>
> O Security Hub retirou esse controle em abril de 2024. Para ter mais informações, consulte Log de alterações dos controles do Security Hub.

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `sns-topic-message-delivery-notification-enabled`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se o registro em log está habilitado para o status de entrega de mensagens de notificação enviadas para um tópico do Amazon SNS para endpoints. Esse controle falhará se a notificação do status de entrega das mensagens não estiver ativada.

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e o desempenho do . O registro de status de entrega de mensagens proporciona um melhor insight operacional, por exemplo:

- Saber se uma mensagem foi entregue para o endpoint do Amazon SNS.
- Identificar a resposta enviada do endpoint do Amazon SNS ao Amazon SNS.
- Determinar o tempo de permanência da mensagem (o tempo entre o carimbo de data e hora da publicação e antes do envio para um endpoint do Amazon SNS).

Correção

Para configurar o registro do status de entrega para um tópico, consulte Status de entrega de mensagens do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

[SNS.3] Os tópicos do SNS devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-sns-topic` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se um tópico do Amazon SNS tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se o tópico não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o tópico não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS

Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um tópico do SNS, consulte Configuração de tags de tópico do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.

Amazon Simple Queue Service

Esses controles estão relacionados aos recursos da API de Gateway.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

As filas do Amazon SQS devem ser criptografadas em repouso

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Proteção de dados > Criptografia de dados em repouso

Severidade: média

Tipo de recurso

Regra AWS Config : `sqs-queue-encrypted` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma fila do Amazon SQS está criptografada em repouso. O controle falhará se a fila não for criptografada com uma chave gerenciada pelo SQS (SSE-SQS) ou uma AWS Key Management Service chave () (SSE-KMS).AWS KMS

Criptografar dados em repouso reduz o risco de um usuário não autorizado acessar os dados armazenados em disco. A criptografia do lado do servidor (SSE) protege o conteúdo das mensagens nas filas do SQS usando chaves de criptografia gerenciadas pelo SQS (SSE-SQS) ou chaves (SSE-KMS). AWS KMS

Correção

Para configurar o SSE para uma fila SQS, consulte Configuração da criptografia do lado do servidor (SSE) para uma fila (console) no Amazon Simple Queue Service Developer Guide.

[SQS.2] As filas SQS devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-sqs-queue` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	`No default value`

Esse controle verifica se uma fila do Amazon SQS tem tags com as chaves específicas definidas no parâmetro. `requiredTagKeys` O controle falhará se a fila não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a fila não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou

outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma fila existente usando o console do Amazon SQS, consulte Configuração de tags de alocação de custos para uma fila do Amazon SQS (console) no Guia do desenvolvedor do Amazon Simple Queue Service.

AWS Step Functions controles

Esses controles estão relacionados aos recursos do Step Functions.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[StepFunctions.1] As máquinas de estado do Step Functions devem ter o registro ativado

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `step-functions-state-machine-logging-enabled`

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`logLevel`	Nível mínimo de registro em log	Enum	`ALL`, `ERROR`, `FATAL`	Nenhum valor padrão

Isso controla se uma máquina de AWS Step Functions estado tem o registro ativado. O controle falhará se uma máquina de estado não tiver o registro em log ativado. Se você fornecer um valor personalizado para o parâmetro `logLevel`, o controle passará somente se a máquina de estados tiver o nível de registro em log especificado ativado.

O monitoramento ajuda a manter a confiabilidade, a disponibilidade e a performance do Step Functions. Você deve coletar o máximo de dados de monitoramento Serviços da AWS que você usa para poder depurar falhas de vários pontos com mais facilidade. Ter uma configuração de registro definida para suas máquinas de estado do Step Functions permite que você acompanhe o histórico de execução e os resultados no Amazon CloudWatch Logs. Opcionalmente, é possível rastrear somente erros ou eventos fatais.

Correção

Para ativar o registro em log em uma máquina de estado do Step Functions, consulte Configurar registro em log no Guia do desenvolvedor do AWS Step Functions .

[StepFunctions.2] As atividades do Step Functions devem ser marcadas

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

AWS Config regra: `tagged-stepfunctions-activity` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.	StringList	Lista de tags que atendem aos AWS requisitos	Nenhum valor padrão

Esse controle verifica se uma AWS Step Functions atividade tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se a atividade não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se a atividade não estiver marcada com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a uma atividade do Step Functions, consulte Marcação em Step Functions no Guia do AWS Step Functions desenvolvedor.

AWS Transfer Family controles

Esses controles estão relacionados aos recursos da Transfer Family.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

Os AWS Transfer Family fluxos de trabalho [Transfer.1] devem ser marcados

Categoria: Identificar > Inventário

Severidade: baixa

Tipo de recurso

Regra AWS Config : `tagged-transfer-workflow` (regra personalizada do Security Hub)

Tipo de programação: acionado por alterações

Parâmetros:

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
`requiredTagKeys`	Lista de chaves de tag que não são do sistema que o	StringList	Lista de tags que atendem	`No default value`

Parâmetro	Descrição	Tipo	Valores personalizados permitidos	Valor padrão do Security Hub
	recurso avaliado deve conter. Chaves de tag fazem distinção entre maiúsculas e minúsculas.		aos AWS requisitos	

Esse controle verifica se um AWS Transfer Family fluxo de trabalho tem tags com as chaves específicas definidas no parâmetro`requiredTagKeys`. O controle falhará se o fluxo de trabalho não tiver nenhuma chave de tag ou se não tiver todas as chaves especificadas no parâmetro`requiredTagKeys`. Se o parâmetro `requiredTagKeys` não for fornecido, o controle só verificará a existência de uma chave de tag e falhará se o fluxo de trabalho não estiver marcado com nenhuma chave. As tags do sistema, que são aplicadas automaticamente e começam com`aws:`, são ignoradas.

Uma tag é um rótulo que você atribui a um AWS recurso e consiste em uma chave e um valor opcional. Você pode criar tags para categorizar recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ajudar você a identificar, organizar, pesquisar e filtrar recursos. A marcação também ajuda você a rastrear os proprietários de recursos responsáveis por ações e notificações. Ao usar a marcação, você pode implementar o controle de acesso baseado em atributos (ABAC) como uma estratégia de autorização, que define permissões com base em tags. Você pode anexar tags às entidades do IAM (usuários ou funções) e aos AWS recursos. Você pode criar uma única política ABAC ou um conjunto separado de políticas para seus diretores do IAM. Você pode criar essas políticas ABAC para permitir operações quando a tag do diretor corresponder à tag do recurso. Para obter mais informações, consulte Para que serve o ABAC? AWS no Guia do usuário do IAM.

> **Note**
>
> Não adicione informações de identificação pessoal (PII) ou outras informações confidenciais ou sigilosas nas tags. As tags são acessíveis a muitos Serviços da AWS, inclusive AWS Billing. Para obter mais práticas recomendadas de marcação, consulte Como marcar seus AWS recursos no. Referência geral da AWS

Correção

Para adicionar tags a um fluxo de trabalho do Transfer Family (console)

1. Abra o AWS Transfer Family console.
2. No painel de navegação, escolha Fluxos de trabalho. Em seguida, selecione o fluxo de trabalho que você deseja marcar.
3. Escolha Gerenciar tags e adicione as tags.

[Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints

Requisitos relacionados: NIST.800-53.r5 CM-7, NIST.800-53.r5 IA-5, Nist.800-53.r5 SC-8

Categoria: Proteger > Proteção de dados > Criptografia de dados em trânsito

Severidade: média

Tipo de recurso

Regra do AWS Config : `transfer-family-server-no-ftp`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se um AWS Transfer Family servidor usa um protocolo diferente de FTP para conexão de endpoint. O controle falhará se o servidor usar o protocolo FTP para que um cliente se conecte ao endpoint do servidor.

O FTP (File Transfer Protocol) estabelece a conexão do endpoint por meio de canais não criptografados, deixando os dados enviados por esses canais vulneráveis à interceptação. Usar o SFTP (SSH File Transfer Protocol), o FTPS (File Transfer Protocol Secure) ou o AS2 (Applicability Statement 2) oferece uma camada extra de segurança ao criptografar seus dados em trânsito e pode ser usado para ajudar a impedir que possíveis invasores usem ataques semelhantes para espionar person-in-the-middle ou manipular o tráfego da rede.

Correção

Para modificar o protocolo de um servidor Transfer Family, consulte Editar os protocolos de transferência de arquivos no Guia AWS Transfer Family do usuário.

AWS WAF controles

Esses controles estão relacionados aos AWS WAF recursos.

Esses controles podem não estar disponíveis em todos Regiões da AWS. Para ter mais informações, consulte Disponibilidade de controles por região.

[WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

Regra do AWS Config : `waf-classic-logging-enabled`

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o registro está habilitado para uma ACL da web AWS WAF global. Esse controle falhará se o registro em log não estiver habilitado para a ACL da web.

O registro em log é uma parte importante para manter a confiabilidade, a disponibilidade e o desempenho AWS WAF global. É um requisito comercial e de conformidade em muitas organizações e permite solucionar problemas de comportamento de aplicativos. Ele também fornece informações detalhadas sobre o tráfego que é analisado pela ACL da web que está associada ao AWS WAF.

Correção

Para ativar o registro de uma ACL AWS WAF da web, consulte Registro de informações de tráfego da ACL da web no Guia do AWS WAF desenvolvedor.

[WAF.2] As regras regionais AWS WAF clássicas devem ter pelo menos uma condição

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso

Regra do AWS Config : `waf-regional-rule-not-empty`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma regra AWS WAF regional tem pelo menos uma condição. O controle falhará se nenhuma condição estiver presente em uma regra.

Uma regra regional do WAF pode conter várias condições. As condições da regra permitem a inspeção do tráfego e a execução de uma ação definida (permitir, bloquear ou contar). Sem quaisquer condições, o tráfego passa sem inspeção. Uma regra regional do WAF sem condições, mas com um nome ou etiqueta sugerindo permitir, bloquear ou contar, pode levar à suposição errada de que uma dessas ações está ocorrendo.

Correção

Para adicionar uma condição a uma regra vazia, consulte Adicionar e remover condições em uma regra no Guia do desenvolvedor do AWS WAF .

[WAF.3] Os grupos de regras regionais AWS WAF clássicos devem ter pelo menos uma regra

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso

Regra do AWS Config : `waf-regional-rulegroup-not-empty`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um grupo de regras AWS WAF regionais tem pelo menos uma regra. O controle falhará se não houver regras no grupo de regras.

Uma regra regional do WAF pode conter várias condições. As condições da regra permitem a inspeção do tráfego e a execução de uma ação definida (permitir, bloquear ou contar). Sem quaisquer condições, o tráfego passa sem inspeção. Uma regra regional do WAF sem condições, mas com um nome ou etiqueta sugerindo permitir, bloquear ou contar, pode levar à suposição errada de que uma dessas ações está ocorrendo.

Correção

Para adicionar regras e condições de regras a um grupo de regras vazio, consulte Adicionar e excluir regras de um grupo de regras AWS WAF clássico e Adicionar e remover condições em uma regra no Guia do AWS WAF desenvolvedor.

[WAF.4] As ACLs regionais AWS WAF clássicas da web devem ter pelo menos uma regra ou grupo de regras

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso

Regra do AWS Config : `waf-regional-webacl-not-empty`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma AWS WAF Classic regional Web ACL contém alguma regra WAF ou grupos de regras WAF. Esse controle falhará se uma ACL da web não contiver nenhuma regra ou grupo de regras do WAF.

Uma ACL da web do WAF Regional pode conter uma coleção de regras e grupos de regras que inspecionam e controlam solicitações da web. Se uma ACL da web estiver vazia, o tráfego da web poderá passar sem ser detectado ou acionado pelo WAF, dependendo da ação padrão.

Correção

Para adicionar regras ou grupos de regras a uma ACL da web regional AWS WAF clássica vazia, consulte Editando uma ACL da Web no Guia do AWS WAF desenvolvedor.

[WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso

Regra do AWS Config : `waf-global-rule-not-empty`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma regra AWS WAF global contém alguma condição. O controle falhará se nenhuma condição estiver presente em uma regra.

Uma regra regional do WAF pode conter várias condições. As condições da regra permitem a inspeção do tráfego e a execução de uma ação definida (permitir, bloquear ou contar). Sem quaisquer condições, o tráfego passa sem inspeção. Uma regra regional do WAF sem condições, mas com um nome ou etiqueta sugerindo permitir, bloquear ou contar, pode levar à suposição errada de que uma dessas ações está ocorrendo.

Correção

Para obter instruções sobre como criar uma regra e adicionar condições, consulte Criar uma regra e adicionar condições no Guia do desenvolvedor do AWS WAF .

[WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso

Regra do AWS Config : `waf-global-rulegroup-not-empty`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se um grupo de regras AWS WAF global tem pelo menos uma regra. O controle falhará se não houver regras no grupo de regras.

Um grupo de regras WAF Global pode conter várias regras. As condições da regra permitem a inspeção do tráfego e a execução de uma ação definida (permitir, bloquear ou contar). Sem quaisquer condições, o tráfego passa sem inspeção. Uma regra regional do WAF sem condições, mas com um nome ou etiqueta sugerindo permitir, bloquear ou contar, pode levar à suposição errada de que uma dessas ações está ocorrendo.

Correção

Para obter instruções sobre como adicionar uma regra a um grupo de regras, consulte Criação de um grupo de regras AWS WAF clássico no Guia do AWS WAF desenvolvedor.

[WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

Requisitos relacionados: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-3(6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-7(10), NIST.800-53.r5 SI-7(6)

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso

Regra do AWS Config : `waf-global-webacl-not-empty`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma Web ACL AWS WAF global contém pelo menos uma regra WAF ou um grupo de regras WAF. Esse controle falhará se uma ACL da web não contiver nenhuma regra ou grupo de regras do WAF.

Uma ACL da web regional do WAF pode conter uma coleção de regras e grupos de regras que inspecionam e controlam solicitações da web. Se uma ACL da web estiver vazia, o tráfego da web poderá passar sem ser detectado ou acionado pelo WAF, dependendo da ação padrão.

Correção

Para adicionar regras ou grupos de regras a uma ACL da web AWS WAF global vazia, consulte Edição de uma ACL da web no Guia do AWS WAF desenvolvedor. Em Filtro, escolha Global (CloudFront).

[WAF.10] as ACLs AWS WAF da web devem ter pelo menos uma regra ou grupo de regras

Requisitos relacionados: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Proteger > Configuração de rede segura

Severidade: média

Tipo de recurso

Regra do AWS Config : `wafv2-webacl-not-empty`

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma lista de controle de acesso à web AWS WAF V2 (Web ACL) contém pelo menos uma regra ou grupo de regras. Esse controle falhará se uma ACL da web não contiver nenhuma regra ou grupo de regras do WAF.

A ACL da web é um recurso que oferece controle detalhado sobre todas as solicitações web HTTP (S) às quais o recurso protegido responde. Uma ACL da web regional do WAF pode conter uma coleção de regras e grupos de regras que inspecionam e controlam solicitações da web. Se uma ACL da web estiver vazia, o tráfego da web poderá passar sem ser detectado ou manipulado, AWS WAF dependendo da ação padrão.

Correção

Para adicionar regras ou grupos de regras a uma ACL da web regional Classic vazia, consulte Editar uma ACL da web no Guia do desenvolvedor do .

[WAF.11] O registro de ACL AWS WAF da web deve estar ativado

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: baixa

Tipo de recurso

AWS Config regra: **`wafv2-logging-enabled`**

Tipo de programação: Periódico

Parâmetros: nenhum

Esse controle verifica se o registro está ativado para uma lista de controle de acesso à web AWS WAF V2 (Web ACL). Esse controle falhará se o registro em log não estiver habilitado para a ACL da web.

O registro mantém a confiabilidade, a disponibilidade e o desempenho do AWS WAF. Além disso, o registro em log é um requisito comercial e de conformidade em muitas organizações. Ao registrar em log o tráfego que é analisado pela sua ACL da web, é possível solucionar problemas de comportamento do aplicativo.

Correção

Para ativar o registro de uma ACL AWS WAF da web, consulte Gerenciando o registro de uma ACL da web no Guia do AWS WAF desenvolvedor.

As AWS WAF regras [WAF.12] devem ter métricas habilitadas CloudWatch

Requisitos relacionados: NIST.800-53.r5 AC-4(26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7(9), NIST.800-53.r5 SI-7(8)

Categoria: Identificar > Registro em log

Severidade: média

Tipo de recurso

AWS Config regra: **`wafv2-rulegroup-logging-enabled`**

Tipo de programação: acionado por alterações

Parâmetros: nenhum

Esse controle verifica se uma AWS WAF regra ou grupo de regras tem CloudWatch métricas da Amazon ativadas. O controle falhará se a regra ou o grupo de regras não tiver CloudWatch métricas ativadas.

A configuração de CloudWatch métricas em AWS WAF regras e grupos de regras fornece visibilidade do fluxo de tráfego. É possível ver quais regras de ACL são acionadas e quais solicitações são aceitas e bloqueadas. Essa visibilidade pode ajudar você a identificar atividades maliciosas nos recursos associados.

Correção

Para ativar CloudWatch métricas em um grupo de AWS WAF regras, invoque a UpdateRuleGroupAPI. Para ativar CloudWatch métricas em uma AWS WAF regra, invoque a API da UpdateWebACL. Veja o campo `CloudWatchMetricsEnabled` no `true`. Quando você usa o AWS WAF console para criar regras ou grupos de regras, as CloudWatch métricas são ativadas automaticamente.

Visualizando e gerenciando padrões de segurança

Um controle é uma proteção dentro de um padrão de segurança que ajuda uma organização a proteger a confidencialidade, integridade e disponibilidade de suas informações. No Security Hub, um controle está relacionado a um AWS recurso específico.

Visualizar controles consolidados

A página Controles do console do Security Hub exibe todos os controles disponíveis no atual Região da AWS (você pode visualizar os controles no contexto de um padrão visitando a página Padrões de segurança e escolhendo um padrão ativado). O Security Hub atribui aos controles um ID, título e descrição de controle de segurança consistentes em todos os padrões. Os IDs de controles incluem o número relevante AWS service (Serviço da AWS) e um número exclusivo (por exemplo, CodeBuild .3).

As informações a seguir estão disponíveis na página Controles do Console do Security Hub:

- Uma pontuação geral de segurança com base na proporção de controles aprovados em comparação com o número total de controles habilitados com dados
- A porcentagem de falhas nas verificações de segurança em todos os controles habilitados
- O número de verificações de segurança que falharam nos controles de cada severidade
- Os controles são divididos em guias diferentes com base no status de ativação. Os controles disponíveis que não se aplicam a nenhum dos seus padrões ativados aparecem na coluna Desativado. Controles não processados, como aqueles que não estão disponíveis na sua região atual, aparecem na coluna Sem dados. O número de controles na coluna Todos habilitados é a soma dos controles nas colunas Falha, Desconhecido, Sem dados e Aprovado.

Na página Controles, é possível escolher um controle para visualizar seus detalhes e agir de acordo com as descobertas geradas pelo controle. Nessa página, você também pode ativar ou desativar um controle de segurança em seu atual Conta da AWS Região da AWS e. As ações de ativação e desativação da página Controles se aplicam a todos os padrões. Para ter mais informações, consulte Ativando e desativando controles no padrão.

Para contas de administrador, a página Controles reflete o status dos controles nas contas dos membros. Se uma verificação de controle falhar em pelo menos uma conta-membro, o controle aparecerá na guia Falha da página Controles. Se você definiu uma Região de agregação, a página Controles refletirá o status dos controles em todas as regiões vinculadas. Se uma verificação de controle falhar em pelo menos uma conta-membro, o controle aparecerá na guia Falha da página Controles.

A exibição de controles consolidados causa alterações nos campos de busca de controle no Formato de descoberta AWS de segurança (ASFF) que podem afetar os fluxos de trabalho. Para ter mais informações, consulte Visualização de controles consolidados — alterações no ASFF.

Pontuação geral de segurança para controles

A página Controles exibe uma pontuação geral de segurança de 0–100%. Uma pontuação geral de segurança com base na proporção de controles aprovados em comparação com o número total de controles habilitados com dados

> **Note**
>
> Para ver a pontuação geral de segurança dos controles, você deve adicionar permissão para chamar **`BatchGetControlEvaluations`** para o perfil do IAM que você usa para acessar o

Security Hub. Essa permissão não é necessária para visualizar as pontuações de segurança de padrões específicos.

Quando você habilita o Security Hub pela primeira vez, o Security Hub calcula a pontuação de segurança resumida e as pontuações de segurança padrão dentro de 30 minutos após sua primeira visita à página Resumo ou à página Padrões de Segurança no console do Security Hub. Pode levar até 24 horas para que as pontuações de segurança pela primeira vez sejam geradas nas regiões da China e AWS GovCloud (US) Region. As pontuações são geradas somente para padrões que são ativados quando você visita essas páginas. Para ver uma lista dos padrões atualmente habilitados, invoque a operação da API `GetEnabledStandards`. Além disso, a gravação de recursos AWS Config deve ser configurada para que o status do controle apareça. A pontuação de segurança resumida é a média das pontuações de segurança padrão.

Após a primeira geração de pontuação, o Security Hub atualiza as pontuações de segurança a cada 24 horas. O Security Hub exibe um timestamp para indicar quando uma pontuação de segurança foi atualizada pela última vez.

Se você definiu uma região de agregação, as pontuações de segurança se aplicam a todas as regiões e incluem descobertas em todas as regiões vinculadas.

Tópicos

Categorias de controle

Cada controle é atribuído a uma categoria. A categoria de um controle reflete a função de segurança à qual o controle se aplica.

O valor da categoria contém a categoria, a subcategoria dentro da categoria e, opcionalmente, um classificador dentro da subcategoria. Por exemplo: .

- Identificar > Inventário
- Categoria: Proteger > Proteção de dados > Criptografia de dados em trânsito

Aqui estão as descrições das categorias, subcategorias e classificadores disponíveis.

Identificar

Desenvolva a compreensão organizacional para gerenciar o risco de segurança cibernética para sistemas, ativos, dados e recursos.

Inventário

O serviço implementou as estratégias corretas de marcação de recursos? As estratégias de marcação incluem o proprietário do recurso?

Quais recursos são usados pelo serviço? Eles são recursos aprovados para este serviço?

Você tem visibilidade do inventário aprovado? Por exemplo, você usa serviços como o Amazon EC2 Systems Manager e o Service Catalog?

Registro em log

Você habilitou com segurança todos os registros em log relevantes para o serviço? São exemplos de evento:

- Logs de fluxo do Amazon VPC
- Logs de acesso do Elastic Load Balancing
- CloudFront Registros da Amazon
- CloudWatch Registros da Amazon
- Amazon Relational Database Service
- Registros de indexação lentos do Amazon OpenSearch Service
- Rastreamento do X-Ray
- AWS Directory Service troncos
- AWS Config itens
- Snapshots

Proteger

Desenvolver e implementar as proteções adequadas para garantir a entrega de serviços críticos de infraestrutura e práticas de programação segura.

Gerenciamento de acesso seguro

- O serviço usa práticas de privilégio mínimo em políticas do ou de recursos?
- As senhas e os segredos são suficientemente complexos? Eles são alternados de maneira apropriada?
- O serviço usa autenticação multifator (MFA)?
- O serviço evita a conta raiz?
- As políticas baseadas em recursos permitem acesso público?

Configuração de rede segura

- O serviço evita acesso remoto público e inseguro à rede?
- O serviço usa VPCs corretamente? Por exemplo, os trabalhos precisam ser executados em VPCs?
- O serviço segmenta e isola adequadamente recursos confidenciais?

Proteção de dados

- Criptografia de dados em repouso — O serviço criptografa dados em repouso?
- Criptografia de dados em trânsito — O serviço criptografa dados em trânsito?
- Integridade dos dados — O serviço valida a integridade dos dados?
- Proteção contra exclusão de dados — O serviço protege os dados contra exclusão acidental?
- Gerenciamento e uso de dados — Você usa serviços como o Amazon Macie para rastrear a localização de seus dados confidenciais?

Proteção de APIs

- O serviço é usado AWS PrivateLink para proteger as operações da API do serviço?

Serviços de proteção

Os serviços de proteção corretos estão em vigor? Eles fornecem a quantidade correta de cobertura?

Os serviços de proteção ajudam você a desviar ataques e comprometimentos direcionados ao serviço. Exemplos de serviços de proteção AWS incluem AWS Control Tower,, AWS WAF AWS Shield Advanced, Vanta, Secrets Manager, IAM Access Analyzer e. AWS Resource Access Manager

Desenvolvimento seguro

Você usa práticas de programação segura?

Você evita vulnerabilidades como os Open Web Application Security Project (OWASP) Top Ten?

Detectar

Desenvolver e implementar as atividades adequadas para identificar a ocorrência de um evento de segurança cibernética.

Serviços de detecção

Os serviços de detecção corretos estão em vigor?

Eles fornecem a quantidade correta de cobertura?

Exemplos de serviços de AWS detecção incluem Amazon GuardDuty AWS Security Hub, Amazon Inspector, Amazon Detective, CloudWatch Amazon Alarms e. AWS IoT Device Defender AWS Trusted Advisor

Resposta

Desenvolver e implementar as atividades adequadas para tomar medidas em relação a um evento de segurança cibernética detectado.

Ações de resposta

Você responde rapidamente aos eventos de segurança?

Você tem alguma descoberta crítica ativa ou de alta gravidade?

Dados forenses

É possível adquirir com segurança dados forenses para o serviço? Por exemplo, você adquire instantâneos do associados a descobertas positivas verdadeiras?

Você configurou uma conta de dados forenses?

Recuperar

Desenvolver e implementar as atividades adequadas para manter planos de resiliência e restaurar quaisquer recursos ou serviços que tenham sido prejudicados devido a um evento de segurança cibernética.

Resiliência

A configuração do serviço oferece suporte a failovers ágeis, dimensionamento elástico e alta disponibilidade?

Você estabeleceu backups?

Ativando e desativando controles no padrão

AWS Security Hub gera descobertas para controles ativados e considera todos os controles ativados ao calcular as pontuações de segurança. É possível escolher habilitar e desabilitar os controles em todos os padrões de segurança ou configurar o status de habilitação de forma diferente em padrões diferentes. Recomendamos a primeira opção, na qual o status de habilitação de um controle está alinhado com todos os padrões habilitados. Esta seção explica como habilitar e desabilitar controles em vários padrões. Para habilitar ou desabilitar um controle em um ou mais padrões específicos, consulte Ativando e desativando controles no padrão.

Se você tiver definido uma região de agregação, o console do Security Hub exibirá controles de todas as regiões vinculadas. Se um controle estiver disponível em uma região vinculada, mas não na região de agregação, você não poderá habilitar ou desabilitar esse controle na região de agregação.

> **Note**
>
> As instruções para habilitar e desabilitar os controles variam de acordo com o uso ou não da configuração central. Esta seção descreve as diferenças. A configuração central está

disponível para usuários que integram o Security Hub AWS Organizations e. Recomendamos usar a configuração central para simplificar o processo de habilitação e desabilitação de controles em ambientes com várias contas e várias regiões.

Habilitação de controles

Quando você habilita um controle em um padrão, o Security Hub começa a executar verificações de segurança para o controle e a gerar descobertas para o controle.

O Security Hub inclui o status do controle no cálculo da pontuação de segurança do padrão. Se você ativar as descobertas de controle consolidadas, receberá uma única descoberta para uma verificação de segurança, mesmo que tenha habilitado um controle em vários padrões. Para obter mais informações, consulte Descobertas de controle consolidadas.

Habilitação de um controle em todos os padrões em várias contas e regiões

Para habilitar um controle de segurança em várias contas Regiões da AWS, você deve usar a configuração central.

Quando você usa a configuração central, o administrador delegado pode criar políticas de configuração do Security Hub que habilitem controles específicos em padrões habilitados. Em seguida, é possível associar a política de configuração a contas e unidades organizacionais (OUs) específicas ou à raiz. Uma política de configuração entra em vigor na sua região inicial (também chamada de região de agregação) e em todas as regiões vinculadas.

As políticas de configuração oferecem personalização. Por exemplo, é possível optar por habilitar todos os controles em uma OU e optar por habilitar somente os controles do Amazon Elastic Compute Cloud (EC2) em outra OU. O nível de granularidade depende das metas pretendidas para a cobertura de segurança em sua organização. Para obter instruções sobre como criar uma política de configuração que habilite controles específicos em padrões, consulte Criação e associação de políticas de configuração do Security Hub.

> **Note**
>
> O administrador delegado pode criar políticas de configuração para gerenciar controles em todos os padrões, exceto o Padrão Gerenciado por Serviços:. AWS Control Tower Os controles desse padrão devem ser configurados no AWS Control Tower serviço.

Se você quiser que algumas contas configurem seus próprios controles em vez do administrador delegado, o administrador delegado pode designar essas contas como autogerenciadas. As contas autogerenciadas devem configurar controles separadamente em cada região.

Habilitação de um controle em todos os padrões em uma única conta e região

Se você não usar a configuração central ou se for uma conta autogerenciada, não será possível usar políticas de configuração para habilitar controles de forma centralizada em várias contas e regiões. Contudo, é possível usar as etapas a seguir para habilitar um controle em uma única conta e região.

Security Hub console

Para habilitar um controle em padrões em uma conta e região

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Roles (Funções).
3. Escolha a guia Desativado.
4. Escolha a opção ao lado de um controle.
5. Escolha Ativar controle (essa opção não aparece para um controle que já está ativado).
6. Repita em cada região na qual deseja habilitar o controle.

Security Hub API

Para habilitar um controle em padrões em uma conta e região

1. Invoque a API ListStandardsControlAssociations. Forneça uma ID de controle de segurança.

   Exemplo de solicitação

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. Invoque a API BatchUpdateStandardsControlAssociations. Forneça o Nome do recurso da Amazon (ARN) do padrão que deseja habilitar. Para obter o ARN padrão, execute `DescribeStandards`.
3. Defina o parâmetro `AssociationStatus` como `ENABLED`. Se você seguir essas etapas para um controle que já está desativado, a API retornará uma resposta do código de status HTTP 200.

Exemplo de solicitação

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]
}
```

4. Repita em cada região na qual deseja habilitar o controle.

AWS CLI

Para habilitar um controle em padrões em uma conta e região

1. Execute o comando list-standards-control-associations. Forneça uma ID de controle de segurança.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Execute o comando batch-update-standards-control-associations. Forneça o Nome do recurso da Amazon (ARN) do padrão que deseja habilitar. Para obter o ARN padrão, execute `describe-standards`.
3. Defina o parâmetro `AssociationStatus` como `ENABLED`. Se você seguir essas etapas para um controle que já está desativado, a API retornará uma resposta do código de status HTTP 200.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0", "AssociationStatus": "ENABLED"}]'
```

4. Repita em cada região na qual deseja habilitar o controle.

Habilitação de Habilitação de novos controles em padrões habilitados.

O Security Hub lança regularmente novos controles de segurança e os adiciona a um ou mais padrões. É possível escolher se deseja habilitar automaticamente novos controles nos padrões habilitados.

> **Note**
>
> Recomendamos usar a configuração central para habilitar automaticamente novos controles. Se sua política de configuração incluir uma lista de controles a serem desabilitados (programaticamente, isso reflete o `DisabledSecurityControlIdentifiers` parâmetro), o Security Hub habilita automaticamente todos os outros controles em todos os padrões, incluindo os controles recém-lançados. Se sua política incluir uma lista de controles a serem habilitados (isso reflete o parâmetro `EnabledSecurityControlIdentifiers`), o Security Hub desabilitará automaticamente todos os outros controles nos padrões, incluindo os controles recém-lançados. Para ter mais informações, consulte Como as políticas de configuração do Security Hub funcionam.

Escolha seu método de acesso preferido e siga estas etapas para ativar um padrão. As etapas a seguir se aplicam somente caso você não use a configuração central.

Security Hub console

Para habilitar automaticamente novos controles

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, selecione Configurações e em seguida Contas.
3. Em Controles, escolha Editar.
4. Ative a Ativação automática de novos controles nos padrões habilitados.
5. Escolha Salvar.

Security Hub API

Para habilitar automaticamente novos controles

1. Invoque a API UpdateSecurityHubConfiguration.

2. Para ativar automaticamente novos controles para os padrões habilitados, defina `AutoEnableControls` como `true`. Se você não quiser habilitar automaticamente novos controles, defina `AutoEnableControls` como false.

AWS CLI

Para habilitar automaticamente novos controles

1. Execute o comando update-security-hub-configuration.
2. Para ativar automaticamente novos controles para os padrões habilitados, defina como . Se você não quiser habilitar automaticamente novos controles, defina `--no-auto-enable-controls` como false.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

Exemplo de comando da

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

Desabilitação de controles

Quando você desabilita um controle em todos os padrões, ocorre o seguinte:

- As verificações de segurança do controle não são mais realizadas para esse padrão.
- Não são geradas descobertas adicionais para esse controle.
- As descobertas existentes são arquivadas automaticamente após três a cinco dias (observe que esse é o melhor esforço).
- Todas AWS Config as regras relacionadas criadas pelo Security Hub são removidas.

Em vez de desabilitar um controle em todos os padrões, é possível simplesmente desabilitar o controle em um ou mais padrões específicos. Se você fizer isso, o Security Hub não executará verificações de segurança para o controle dos padrões nos quais você o desabilitou, portanto, isso não afetará a pontuação de segurança desses padrões. No entanto, o Security Hub mantém a AWS Config regra e continua executando verificações de segurança para o controle, se ele estiver habilitado em outros padrões. Isso pode afetar sua pontuação de segurança resumida. Para obter

instruções sobre como configurar controles em padrões específicos, consulte Ativando e desativando controles no padrão.

Para reduzir o ruído de localização, pode ser útil desativar os controles que não são relevantes para o seu ambiente. Para obter recomendações sobre quais controles desabilitar, consulte Controles do Security Hub que você pode querer desabilitar.

Quando você desabilita um padrão, todos os controles que se aplicam ao padrão são desabilitados (no entanto, esses controles ainda podem permanecer habilitados em outros padrões). Para obter mais informações sobre como desativar as ACLs, consulte the section called “Habilitar e desabilitar as SCPs”.

Quando você desativa um padrão, o Security Hub não rastreia quais dos controles aplicáveis foram desativados. Se você reativar posteriormente o mesmo padrão, todos os controles que se aplicam a ele serão ativados automaticamente. Além disso, desativar um controle não é uma ação permanente. Suponha que você desabilite um controle e, em seguida, habilite um padrão que tenha sido desabilitado anteriormente. Se o padrão incluir esse controle, ele será ativado nesse padrão. Quando você ativa um padrão, o Security Hub ativa automaticamente os controles que se aplicam ao padrão. Você pode optar por desativar controles específicos.

Desabilitação de um controle em todos os padrões em várias contas e regiões

Para desativar um controle de segurança em várias contas Regiões da AWS, você deve usar a configuração central.

Quando você usa a configuração central, o administrador delegado pode criar políticas de configuração do Security Hub que desabilitem controles específicos em padrões habilitados. Em seguida, é possível associar a política de configuração a contas específicas, ou à raiz. Uma política de configuração entra em vigor na sua região inicial (também chamada de região de agregação) e em todas as regiões vinculadas.

As políticas de configuração oferecem personalização. Por exemplo, você pode optar por desativar todos os AWS CloudTrail controles em uma OU e pode optar por desativar todos os controles do IAM em outra OU. O nível de granularidade depende das metas pretendidas para a cobertura de segurança em sua organização. Para obter instruções sobre como criar uma política de configuração que desabilite controles específicos em padrões, consulte Criação e associação de políticas de configuração do Security Hub.

> **Note**
>
> O administrador delegado pode criar políticas de configuração para gerenciar controles em todos os padrões, exceto o Padrão Gerenciado por Serviços:. AWS Control Tower Os controles desse padrão devem ser configurados no AWS Control Tower serviço.

Se você quiser que algumas contas configurem seus próprios controles em vez do administrador delegado, o administrador delegado pode designar essas contas como autogerenciadas. As contas autogerenciadas devem configurar controles separadamente em cada região.

Desabilitação de um controle em todos os padrões em uma única conta e região

Se você não usar a configuração central ou se for uma conta autogerenciada, não será possível usar políticas de configuração para desabilitar controles de forma centralizada em várias contas e regiões. Contudo, é possível usar as etapas a seguir para desabilitar um controle em uma única conta e região.

Security Hub console

Para desabilitar um controle em padrões em uma conta e região

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Roles (Funções).
3. Escolha a opção ao lado de um controle.
4. Escolha Ativar controle (essa opção não aparece para um controle que já está ativado).
5. Forneça um motivo para desativar o controle e confirme escolhendo Desativar.
6. Repita em cada região na qual deseja desabilitar o controle.

Security Hub API

Para desabilitar um controle em padrões em uma conta e região

1. Invoque a API ListStandardsControlAssociations. Forneça uma ID de controle de segurança.

   Exemplo de solicitação

   ```
   {
   ```

```
    "SecurityControlId": "IAM.1"
}
```

2. Invoque a API BatchUpdateStandardsControlAssociations. Forneça o ARN do padrão no qual você deseja ativar o controle. Para obter o ARN padrão, execute `DescribeStandards`.
3. Defina o parâmetro `AssociationStatus` como `DISABLED`. Se você seguir essas etapas para um controle que já está desativado, a API retornará uma resposta do código de status HTTP 200.

   Exemplo de solicitação

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not
 applicable to environment"}, {"SecurityControlId": "IAM.1", "StandardsArn":
 "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/
v/1.0.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}}]
}
```

4. Repita em cada região na qual deseja desabilitar o controle.

AWS CLI

Para desabilitar um controle em padrões em uma conta e região

1. Execute o comando list-standards-control-associations. Forneça uma ID de controle de segurança.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Execute o comando batch-update-standards-control-associations. Forneça o ARN do padrão no qual você deseja ativar o controle. Para obter o ARN padrão, execute `describe-standards`.
3. Defina o parâmetro `AssociationStatus` como `DISABLED`. Se você seguir essas etapas para um controle que já está desativado, a API retornará uma resposta do código de status HTTP 200.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable
 to environment"}, {"SecurityControlId": "CloudTrail.1", "StandardsArn":
 "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/v/1.4.0",
 "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}]'
```

4. Repita em cada região na qual deseja desabilitar o controle.

Para obter mais informações, consulte Habilitação de novos controles em padrões habilitados automaticamente.

AWS Security Hub libera regularmente novos controles e os adiciona a um ou mais padrões. É possível escolher se deseja habilitar automaticamente novos controles nos padrões habilitados.

> **Note**
>
> Se você usar a configuração central e incluir uma lista de controles específicos a serem desabilitados em sua política de configuração (programaticamente, isso reflete o parâmetro `DisabledSecurityControlIdentifiers`), o Security Hub habilitará automaticamente todos os outros controles em todos os padrões, incluindo controles recém-lançados. Para ter mais informações, consulte Como as políticas de configuração do Security Hub funcionam.

Recomendamos usar a configuração central do Security Hub para habilitar automaticamente novos controles de segurança. É possível criar políticas de configuração que incluam uma lista de controles a serem desabilitados em todos os padrões. Todos os outros controles, incluindo os recém-lançados, são habilitados por padrão. De forma alternativa, é possível criar políticas que incluam uma lista de controles a serem habilitados nos padrões. Todos os outros controles, incluindo os recém-lançados, são desabilitados por padrão. Para ter mais informações, consulte Como a configuração central funciona.

O Security Hub não habilita novos controles quando eles são adicionados a um padrão que você não habilitou.

As etapas a seguir se aplicam somente caso você não use a configuração central.

Escolha seu método de acesso preferido e siga estas etapas para ativar um padrão.

Security Hub console

Para habilitar automaticamente novos controles

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, selecione Configurações e em seguida Contas.
3. Em Controles, escolha Editar.
4. Ative a Ativação automática de novos controles nos padrões habilitados.
5. Escolha Salvar.

Security Hub API

Para habilitar automaticamente novos controles

1. Executar `UpdateSecurityHubConfiguration`.
2. Para ativar automaticamente novos controles para os padrões habilitados, defina `AutoEnableControls` como `true`. Se você não quiser habilitar automaticamente novos controles, defina `AutoEnableControls` como false.

AWS CLI

Para habilitar automaticamente novos controles

1. Execute o comando `update-security-hub-configuration`.
2. Para ativar automaticamente novos controles para os padrões habilitados, defina como . Se você não quiser habilitar automaticamente novos controles, defina `--no-auto-enable-controls` como false.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

Exemplo de comando da

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

Se você não habilitar automaticamente os novos controles, deverá habilitá-los manualmente. Para obter instruções, consulte the section called “Ativando e desativando controles no padrão”.

Parâmetros de controle personalizados

Alguns controles do Security Hub usam parâmetros que afetam a forma como o controle é avaliado. Normalmente, esses controles são avaliados em relação aos valores de parâmetros padrão definidos pelo Security Hub. Entretanto, para um subconjunto desses controles, é possível personalizar os valores dos parâmetros. Quando você personaliza um valor de parâmetro para um controle, o Security Hub começa a avaliar o controle em relação ao valor que você especifica. Se o recurso subjacente ao controle satisfizer o valor personalizado, o Security Hub gerará uma descoberta `PASSED`. Se o recurso não satisfizer o valor personalizado, o Security Hub gerará uma descoberta `FAILED`.

Ao personalizar os parâmetros de controle, é possível refinar as melhores práticas de segurança recomendadas e monitoradas pelo Security Hub para se alinharem aos requisitos de sua empresa e às expectativas de segurança. Em vez de suprimir as descobertas de um controle, é possível personalizar um ou mais de seus parâmetros para obter descobertas que atendam às suas necessidades de segurança.

Aqui estão alguns exemplos de casos de uso para parâmetros de controle personalizados:

- [CloudWatch.16] — os grupos de CloudWatch registros devem ser mantidos por um período de tempo especificado

  É possível especificar o período de tempo de retenção.
- [IAM.7]: as políticas de senha para usuários do IAM devem ter configurações fortes

  É possível especificar parâmetros relacionados à força da senha.
- EC2.18]: os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas

  É possível especificar quais portas estão autorizadas a permitir tráfego de entrada irrestrito.
- [Lambda.5]: as funções do Lambda da VPC devem operar em várias zonas de disponibilidade

É possível especificar o número mínimo de zonas de disponibilidade que produzem uma descoberta aprovada.

Esta seção explica como personalizar e gerenciar parâmetros de controle.

Como os parâmetros de controle personalizados funcionam

Um controle pode ter um ou mais parâmetros personalizáveis. Os possíveis tipos de dados para parâmetros de controle individuais incluem o seguinte:

- Booleano
- Double
- Enum
- EnumList
- Inteiro
- IntegerList
- String
- StringList

Para alguns controles, os valores de parâmetros aceitáveis também devem estar em um intervalo especificado para serem válidos. Nesses casos, o Security Hub fornece o intervalo aceitável.

O Security Hub escolhe valores de parâmetros padrão e pode ocasionalmente atualizá-los. Depois de personalizar um parâmetro de controle, seu valor continua sendo o valor que você especificou para o parâmetro, a menos que você o altere. Ou seja, o parâmetro interrompe o acompanhamento de atualizações no valor padrão do Security Hub, mesmo que o valor personalizado do parâmetro corresponda ao valor padrão atual definido pelo Security Hub. Aqui está um exemplo para o controle [ACM.1]: certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado:

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
```

```
                "Integer": 30
            }
        }
    }
}
```

No exemplo anterior, o parâmetro `daysToExpiration` tem um valor personalizado de `30`. O valor padrão atual desse parâmetro também é `30`. Se o Security Hub alterar o valor padrão para `14`, o parâmetro neste exemplo não acompanhará essa alteração. Ele manterá um valor de `30`.

Se você quiser acompanhar as atualizações do valor padrão do Security Hub para um parâmetro, defina o campo `ValueType` como `DEFAULT` em vez de `CUSTOM`. Para ter mais informações, consulte Reversão para valores padrão dos parâmetros em uma única conta e região.

Ao alterar o valor de um parâmetro, você também aciona uma nova verificação de segurança que avaliará o controle com base no novo valor. Em seguida, o Security Hub gerará novas descobertas de controle com base no novo valor. Durante atualizações periódicas para controlar as descobertas, o Security Hub também usará o novo valor do parâmetro. Se você alterar os valores dos parâmetros de um controle, mas não tiver habilitado nenhum padrão que inclua o controle, o Security Hub não realizará nenhuma verificação de segurança usando os novos valores. Você precisa habilitar pelo menos um padrão relevante para que o Security Hub avalie o controle com base no novo valor do parâmetro.

Os valores de parâmetros personalizados se aplicam a todos os padrões habilitados. Você não pode personalizar os parâmetros de um controle que não seja compatível com sua região atual. Para obter uma lista de limites regionais para controles individuais, consulte Limites regionais de controles.

Personalização de parâmetros de controle

As instruções para personalizar os parâmetros de controle variam de acordo com seu uso da configuração central. A configuração central é um recurso que o administrador delegado do Security Hub pode usar para gerenciar os recursos do Security Hub em Regiões da AWS contas e unidades organizacionais (OUs) em sua organização.

Se sua organização usa a configuração central, o administrador delegado pode criar políticas de configuração que incluam parâmetros de controle personalizados. Essas políticas podem ser associadas a contas-membro e OUs gerenciadas centralmente e entram em vigor na sua região inicial e em todas as regiões vinculadas. O administrador delegado também pode designar uma ou mais contas como autogerenciadas, o que permite que o proprietário da conta configure seus

próprios parâmetros separadamente em cada região. Se sua organização não usa a configuração central, você deverá personalizar os parâmetros de controle separadamente em cada conta e região.

Personalização de parâmetros de controle em várias contas e regiões

Ao usar a configuração central, é possível personalizar os parâmetros de controle para contas e OUs gerenciadas centralmente em várias contas e regiões. Recomendamos usar a configuração central porque ela permite alinhar os valores dos parâmetros de controle em diferentes partes da sua organização. Por exemplo, todas as suas contas de teste podem usar determinados valores de parâmetros, e todas as contas de produção podem usar valores diferentes.

Se você for o administrador delegado do Security Hub de uma organização que use a configuração central, escolha seu método preferido e siga as etapas para personalizar os parâmetros de controle em várias contas e regiões.

Security Hub console

Para personalizar os parâmetros de controle em várias contas e regiões

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

   Certifique-se de que você está conectado à região inicial.
2. No painel de navegação, escolha Configurações e Configuração.
3. Escolha a guia Políticas.
4. Para criar uma nova política de configuração que inclua parâmetros personalizados, escolha Criar política. Para especificar parâmetros personalizados em uma política de configuração existente, selecione a política e escolha Editar.

   Para criar uma nova política de configuração com parâmetros personalizados

   1. Na seção Política personalizada, escolha os padrões e controles de segurança que você deseja habilitar.
   2. Selecione Personalizar parâmetros de controle.
   3. Selecione um controle e, em seguida, especifique valores personalizados para um ou mais parâmetros.
   4. Para personalizar os parâmetros para mais controles, escolha Personalizar controle adicional.
   5. Na seção Contas, selecione as contas ou OUs às quais você deseja aplicar a política.

6. Escolha Próximo.
7. Escolha Criar política e aplicar. Na sua região inicial e em todas as regiões vinculadas, essa ação substitui as configurações existentes das contas e OUs associadas a essa política de configuração. Contas e OUs podem ser associadas a uma política de configuração por meio de aplicação direta ou herança de um pai.

Para adicionar ou editar parâmetros personalizados em uma política de configuração existente

1. Na seção Controles, em Política personalizada, especifique os novos valores de parâmetros personalizados que você deseja.
2. Se essa for a primeira vez que você personaliza parâmetros de controle nessa política, selecione Personalizar parâmetros de controle e, em seguida, selecione um controle para personalizar. Para personalizar os parâmetros para mais controles, escolha Personalizar controle adicional.
3. Na seção Contas, verifique as contas ou OUs às quais você deseja aplicar a política.
4. Escolha Próximo.
5. Revise suas alterações e verifique se estão corretas. Ao terminar, escolha Salvar política e aplicar. Na sua região inicial e em todas as regiões vinculadas, essa ação substitui as configurações existentes das contas e OUs associadas a essa política de configuração. Contas e OUs podem ser associadas a uma política de configuração por meio de aplicação direta ou herança de um pai.

Security Hub API

Para personalizar os parâmetros de controle em várias contas e regiões

Para criar uma nova política de configuração com parâmetros personalizados

1. Invoque a API CreateConfigurationPolicy a partir da conta de administrador delegado na região inicial.
2. Para o objeto `SecurityControlCustomParameters`, forneça o identificador de cada controle que você deseja personalizar.
3. Para o objeto `Parameters`, forneça o nome de cada parâmetro que você deseja personalizar. Para cada parâmetro que você personalizar, forneça `CUSTOM` para `ValueType`. Em `Value`, forneça o tipo de dados do parâmetro e o valor personalizado. O campo `Value`

não poderá estar vazio quando `ValueType` for `CUSTOM`. Se sua solicitação omitir um parâmetro com suporte pelo controle, esse parâmetro reterá seu valor atual. É possível encontrar parâmetros com suporte, tipos de dados e valores válidos para um controle invocando a API GetSecurityControlDefinition.

Para adicionar ou editar parâmetros personalizados em uma política de configuração existente

1. Invoque a API UpdateConfigurationPolicy a partir da conta de administrador delegado na região inicial.
2. No campo `Identifier`, forneça o nome do recurso da Amazon (ARN) ou o ID da política de configuração que deseja atualizar.
3. Para o objeto `SecurityControlCustomParameters`, forneça o identificador de cada controle que você deseja personalizar.
4. Para o objeto `Parameters`, forneça o nome de cada parâmetro que você deseja personalizar. Para cada parâmetro que você personalizar, forneça `CUSTOM` para `ValueType`. Em `Value`, forneça o tipo de dados do parâmetro e o valor personalizado. Se sua solicitação omitir um parâmetro com suporte pelo controle, esse parâmetro reterá seu valor atual. É possível encontrar parâmetros com suporte, tipos de dados e valores válidos para um controle invocando a API GetSecurityControlDefinition.

Exemplo de solicitação de API para criar uma nova política de configuração:

```
{
    "Name": "SampleConfigurationPolicy",
    "Description": "Configuration policy for production accounts",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"},
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"}
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
```

```
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

AWS CLI

Para personalizar os parâmetros de controle em várias contas e regiões

Para criar uma nova política de configuração com parâmetros personalizados

1. Execute o comando create-configuration-policy a partir da conta de administrador delegado na região inicial.
2. Para o objeto `SecurityControlCustomParameters`, forneça o identificador de cada controle que você deseja personalizar.
3. Para o objeto `Parameters`, forneça o nome de cada parâmetro que você deseja personalizar. Para cada parâmetro que você personalizar, forneça `CUSTOM` para `ValueType`. Em `Value`, forneça o tipo de dados do parâmetro e o valor personalizado. O campo `Value` não poderá estar vazio quando `ValueType` for `CUSTOM`. Se sua solicitação omitir um parâmetro com suporte pelo controle, esse parâmetro reterá seu valor atual. É possível encontrar parâmetros com suporte, tipos de dados e valores válidos para um controle executando o comando get-security-control-definition.

Para adicionar ou editar parâmetros em uma política de configuração existente

1. Para adicionar ou atualizar parâmetros de entrada personalizados em uma política de configuração existente, execute o comando update-configuration-policy na conta do administrador delegado na região inicial.
2. No campo `identifier`, forneça o nome do recurso da Amazon (ARN) ou o ID da política que deseja atualizar.
3. Para o objeto `SecurityControlCustomParameters`, forneça o identificador de cada controle que você deseja personalizar.
4. Para o objeto `Parameters`, forneça o nome de cada parâmetro que você deseja personalizar. Para cada parâmetro que você personalizar, forneça `CUSTOM` para `ValueType`. Em `Value`, forneça o tipo de dados do parâmetro e o valor personalizado. Se sua solicitação omitir um parâmetro com suporte pelo controle, esse parâmetro reterá seu valor atual. É possível encontrar parâmetros com suporte, tipos de dados e valores válidos para um controle executando o comando get-security-control-definition.

Exemplo de comando para criar uma nova política de configuração:

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": "Integer": 15}}}]}}'
```

Personalização de parâmetros de controle em uma única conta e região

Se você não usa a configuração central ou tem uma conta autogerenciada, pode personalizar os parâmetros de controle da sua conta em uma região por vez

Escolha seu método preferido e siga as etapas para personalizar os parâmetros de controle. Suas alterações se aplicam somente à sua conta na região atual. Para personalizar os parâmetros de

controle em regiões adicionais, repita as etapas a seguir em cada conta e região adicional na qual você deseja personalizar os parâmetros. O mesmo controle pode usar valores de parâmetros diferentes em regiões diferentes.

Security Hub console

Para personalizar parâmetros de controle em uma conta e região

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Controles. Na tabela, escolha um controle que ofereça suporte a parâmetros personalizados e para o qual você deseja alterar os parâmetros. A coluna Parâmetros personalizados indica quais controles oferecem suporte a parâmetros personalizados.
3. Na página de detalhes do controle, escolha a guia Parâmetros e, em seguida, selecione Editar.
4. Especifique os valores de parâmetros que você desejar.
5. Opcionalmente, na seção Motivo da alteração, selecione um motivo para personalizar os parâmetros.
6. Escolha Salvar.

Security Hub API

Para personalizar parâmetros de controle em uma conta e região

1. Invoque a API UpdateSecurityControl.
2. Em `SecurityControlId`, forneça o ID do controle que você deseja personalizar.
3. Para o objeto `Parameters`, forneça o nome de cada parâmetro que você deseja personalizar. Para cada parâmetro que você personalizar, forneça `CUSTOM` para `ValueType`. Em `Value`, forneça o tipo de dados do parâmetro e o valor personalizado. Se sua solicitação omitir um parâmetro com suporte pelo controle, esse parâmetro reterá seu valor atual.
   É possível encontrar parâmetros com suporte, tipos de dados e valores válidos para um controle invocando a API GetSecurityControlDefinition.
4. Opcionalmente, em `LastUpdateReason`, forneça um motivo para personalizar os parâmetros de controle.

Exemplo de solicitação de API:

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 15
            }
        }
    },
    "LastUpdateReason": "Internal compliance requirement"
}
```

AWS CLI

Para personalizar parâmetros de controle em uma conta e região

1. Execute o comando update-security-control.
2. Em `security-control-id`, forneça o ID do controle que você deseja personalizar.
3. Para o objeto `parameters`, forneça o nome de cada parâmetro que você deseja personalizar. Para cada parâmetro que você personalizar, forneça `CUSTOM` para `ValueType`. Em `Value`, forneça o tipo de dados do parâmetro e o valor personalizado. Se sua solicitação omitir um parâmetro com suporte pelo controle, esse parâmetro reterá seu valor atual. É possível encontrar parâmetros com suporte, tipos de dados e valores válidos para um controle executando o comando get-security-control-definition.
4. Opcionalmente, em `last-update-reason`, forneça um motivo para personalizar os parâmetros de controle.

Exemplo de comando:

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer":
 15}}}' \
--last-update-reason "Internal compliance requirement"
```

Verificação do status dos parâmetros de controle

É importante validar e verificar o status das alterações nos parâmetros de controle. Isso ajuda a garantir que um controle funcione conforme o esperado e forneça o valor de segurança pretendido. Para verificar se a atualização de um parâmetro obteve êxito, é possível revisar os detalhes do controle no console do Security Hub. No console, escolha o controle para exibir seus detalhes. A guia Parâmetros mostra o status da alteração do parâmetro.

Programaticamente, se a sua solicitação para atualizar um parâmetro for válida, o valor do campo `UpdateStatus` será `UPDATING` em resposta à operação BatchGetSecurityControls. Isso significa que a atualização foi válida, mas suas descobertas podem ainda não incluir os valores dos parâmetros atualizados. Quando o valor de `UpdateState` mudar para `READY`, suas descobertas começarão a incluir os valores dos parâmetros atualizados.

A operação `UpdateSecurityControl` retorna uma resposta `InvalidInputException` para valores de parâmetros inválidos. A resposta fornece detalhes adicionais sobre o motivo da falha. Por exemplo, pode ter sido especificado um valor que esteja fora do intervalo válido para um parâmetro. Ou você especificou um valor que não usa o tipo de dados correto. Envie sua solicitação novamente com informações válidas. Se a atualização de um parâmetro não obtiver êxito, o Security Hub reterá o valor atual do parâmetro.

Se ocorrer uma falha interna ao tentar atualizar um valor de parâmetro, o Security Hub tentará novamente automaticamente se você tiver AWS Config ativado. Para ter mais informações, consulte Configurando AWS Config.

Revisando os parâmetros de controle

É possível revisar os valores atuais dos parâmetros de controle individuais em sua conta. Se você usar a configuração central, o administrador delegado do Security Hub também poderá revisar os valores dos parâmetros especificados em uma política de configuração.

Escolha seu método preferido e siga as etapas para revisar os valores atuais dos parâmetros de controle.

Security Hub console

Para revisar os valores dos parâmetros atuais

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Controles. Escolha um controle.

3. Selecione a guia Parâmetros. Essa guia mostra os valores atuais dos parâmetros do controle.

Security Hub API

Para revisar os valores dos parâmetros atuais

Invoque a API BatchGetSecurityControls e forneça um ou mais IDs de controle de segurança ou ARNs. O objeto `Parameters` na resposta mostra os valores dos parâmetros atuais para os controles especificados.

Exemplo de solicitação de API:

```
{
    "SecurityControlIds": ["APIGateway.1", "CloudWatch.15", "IAM.7"]
}
```

AWS CLI

Para revisar os valores dos parâmetros atuais

Execute o comando batch-get-security-controls e forneça um ou mais IDs de controle de segurança ou ARNs. O objeto `Parameters` na resposta mostra os valores dos parâmetros atuais para os controles especificados.

Exemplo de comando:

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

Escolha seu método preferido para visualizar os valores dos parâmetros atuais em uma política de configuração central.

Security Hub console

Para revisar os valores dos parâmetros atuais em uma política de configuração

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

Faça login usando as credenciais da conta do administrador delegado do Security Hub na região inicial.

2. No painel de navegação, escolha Configurações e Configuração.
3. Na guia Políticas, selecione a política de configuração e escolha Exibir detalhes. Em seguida, os detalhes da política serão exibidos, incluindo os valores dos parâmetros atuais.

Security Hub API

Para revisar os valores dos parâmetros atuais em uma política de configuração

1. Invoque a API GetConfigurationPolicy a partir da conta de administrador delegado na região inicial.
2. Forneça o ARN ou o ID da política de configuração cujos detalhes você deseja ver. A resposta inclui valores de parâmetros atuais.

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

Para revisar os valores dos parâmetros atuais em uma política de configuração

1. Execute o comando get-configuration-policy a partir da conta de administrador delegado na região inicial.
2. Forneça o ARN ou o ID da política de configuração cujos detalhes você deseja ver. A resposta inclui valores de parâmetros atuais.

```
$ aws securityhub get-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Suas descobertas de controle também mostram os valores dos parâmetros atuais. Em AWS Sintaxe do Security Finding Format (ASFF), esses valores aparecem no campo `Parameters` do objeto `Compliance`. Para revisar as descobertas no console do Security Hub, escolha Descobertas no painel de navegação. Para revisar as descobertas de forma programática, use a operação GetFindings.

> **Note**
>
> Após o lançamento do recurso de parâmetros de controle personalizados, o Security Hub atualizará as descobertas de controle existentes para incluir o campo do ASFF `Parameters`. Isso pode demorar até 24 horas.

Revertendo para valores de parâmetros de controle padrão

Um parâmetro de controle pode ter um valor padrão definido pelo Security Hub. Podemos atualizar o valor padrão de um parâmetro para refletir a evolução das práticas recomendadas de segurança. Se você não especificou um valor personalizado para um parâmetro de controle, o controle acompanhará automaticamente essas atualizações e usará o novo valor padrão.

É possível voltar a usar valores de parâmetros padrão para um controle. A forma como você faz isso depende se você usa a configuração central.

> **Note**
>
> Nem todos os parâmetros de controle têm um valor padrão no Security Hub. Nesses casos, quando `ValueType` for definido como `DEFAULT`, não haverá um valor padrão específico usado pelo Security Hub. Em vez disso, o Security Hub ignorará o parâmetro na ausência de um valor personalizado.

Reversão para valores de parâmetros padrão em várias contas e regiões

Se você usar a configuração central, poderá reverter os parâmetros de controle para contas e OUs gerenciadas centralmente em várias contas e regiões.

Escolha seu método preferido e siga as etapas para voltar aos valores de parâmetros padrão em várias contas e regiões usando a configuração central.

Security Hub console

Para reverter aos valores padrão dos parâmetros em várias contas e regiões

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

   Faça login usando as credenciais da conta do administrador delegado do Security Hub na região inicial.
2. No painel de navegação, escolha Configurações e Configuração.
3. Escolha a guia Políticas.
4. Selecione uma política e escolha Editar.
5. Em Política personalizada, a seção Controles mostrará uma lista de controles para os quais você especificou parâmetros personalizados.
6. Encontre o controle que tem um ou mais valores de parâmetros a serem revertidos. Em seguida, escolha Remover para reverter aos valores padrão.
7. Na seção Contas, verifique as contas ou OUs às quais você deseja aplicar a política.
8. Escolha Próximo.
9. Revise suas alterações e verifique se estão corretas. Ao terminar, escolha Salvar política e aplicar. Na sua região inicial e em todas as regiões vinculadas, essa ação substitui as configurações existentes das contas e OUs associadas a essa política de configuração. Contas e OUs podem ser associadas a uma política de configuração por meio de aplicação direta ou herança de um pai.

Security Hub API

Para reverter aos valores padrão dos parâmetros em várias contas e regiões

1. Invoque a API UpdateConfigurationPolicy a partir da conta de administrador delegado na região inicial.
2. No campo `Identifier`, forneça o nome do recurso da Amazon (ARN) ou o ID da política que deseja atualizar.
3. Para o objeto `SecurityControlCustomParameters`, forneça o identificador de cada controle para o qual você deseja reverter um ou mais parâmetros.
4. No objeto `Parameters`, para cada parâmetro que você desejar reverter, forneça `DEFAULT` para o campo `ValueType`. Quando `ValueType` estiver definido como `DEFAULT`, você não precisará fornecer um valor para o campo `Value`. Se um valor for incluído na sua solicitação,

o Security Hub o ignorará. Se sua solicitação omitir um parâmetro com suporte pelo controle, esse parâmetro reterá seu valor atual.

> **Warning**
>
> Se você omitir um objeto de controle do campo `SecurityControlCustomParameters`, o Security Hub reverterá todos os parâmetros personalizados do controle para seus valores padrão. Uma lista completamente vazia para `SecurityControlCustomParameters` reverterá os parâmetros personalizados de todos os controles para seus valores padrão.

Exemplo de solicitação de API:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "TestConfigurationPolicy",
    "Description": "Updated configuration policy",
    "UpdatedReason": "Revert ACM.1 parameter to default value",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"},
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"}
                ],
             "SecurityControlsConfiguration": {
                "DisbledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "DEFAULT"
                             }
                         }
```

```
                    }
                ]
            }
        }
    }
}
```

AWS CLI

Para reverter aos valores padrão dos parâmetros em várias contas e regiões

1. Execute o comando update-configuration-policy a partir da conta de administrador delegado na região inicial.
2. No campo `identifier`, forneça o nome do recurso da Amazon (ARN) ou o ID da política que deseja atualizar.
3. Para o objeto `SecurityControlCustomParameters`, forneça o identificador de cada controle para o qual você deseja reverter um ou mais parâmetros.
4. No objeto `Parameters`, para cada parâmetro que você desejar reverter, forneça `DEFAULT` para o campo `ValueType`. Quando `ValueType` estiver definido como `DEFAULT`, você não precisará fornecer um valor para o campo `Value`. Se um valor for incluído na sua solicitação, o Security Hub o ignorará. Se sua solicitação omitir um parâmetro com suporte pelo controle, esse parâmetro reterá seu valor atual.

> **Warning**
>
> Se você omitir um objeto de controle do campo `SecurityControlCustomParameters`, o Security Hub reverterá todos os parâmetros personalizados do controle para seus valores padrão. Uma lista completamente vazia para `SecurityControlCustomParameters` reverterá os parâmetros personalizados de todos os controles para seus valores padrão.

Exemplo de comando:

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
```

```
--name "TestConfigurationPolicy" \
--description "Updated configuration policy" \
--updated-reason "Revert ACM.1 parameter to default value"
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "DEFAULT"}}}]}}'
```

Reversão para valores padrão dos parâmetros em uma única conta e região

Se você não usa a configuração central ou tem uma conta autogerenciada, pode reverter para o uso dos valores padrão dos parâmetros para sua conta em uma região por vez

Escolha seu método preferido e siga as etapas para voltar aos valores padrão dos parâmetros para sua conta em uma única região. Para reverter aos valores padrão dos parâmetros em regiões adicionais, repita essas etapas em cada região adicional.

> **Note**
>
> Se você desabilitar o Security Hub, seus parâmetros de controle personalizados serão redefinidos. Se você habilitar o Security Hub novamente no futuro, todos os controles usarão valores de parâmetros padrão ao iniciar.

Security Hub console

Para reverter aos valores padrão dos parâmetros em uma conta e região

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Controles. Escolha o controle que você deseja reverter para os valores padrão dos parâmetros.
3. Na guia `Parameters`, escolha Personalizado ao lado de um parâmetro de controle. Em seguida, escolha Remover personalização. Esse parâmetro agora usa o valor padrão do Security Hub e acompanhará futuras atualizações até o valor padrão.
4. Repita a etapa anterior para cada valor de parâmetro que desejar reverter.

Security Hub API

Para reverter aos valores padrão dos parâmetros em uma conta e região

1. Invoque a API UpdateSecurityControl.
2. Em `SecurityControlId`, forneça o ARN ou ID do controle cujos parâmetros você deseja reverter.
3. No objeto `Parameters`, para cada parâmetro que você desejar reverter, forneça `DEFAULT` para o campo `ValueType`. Quando `ValueType` estiver definido como `DEFAULT`, você não precisará fornecer um valor para o campo `Value`. Se um valor for incluído na sua solicitação, o Security Hub o ignorará.
4. Opcionalmente, em `LastUpdateReason`, forneça um motivo para reverter aos valores padrão dos parâmetros.

Exemplo de solicitação de API:

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "DEFAULT"
        },
    "LastUpdateReason": "New internal requirement"
}
```

AWS CLI

Para reverter aos valores padrão dos parâmetros em uma conta e região

1. Execute o comando update-security-control.
2. Em `security-control-id`, forneça o ARN ou ID do controle cujos parâmetros você deseja reverter.
3. No objeto `parameters`, para cada parâmetro que você desejar reverter, forneça `DEFAULT` para o campo `ValueType`. Quando `ValueType` estiver definido como `DEFAULT`, você não precisará fornecer um valor para o campo `Value`. Se um valor for incluído na sua solicitação, o Security Hub o ignorará.
4. Opcionalmente, em `last-update-reason`, forneça um motivo para reverter aos valores padrão dos parâmetros.

Exemplo de comando:

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
--last-update-reason "New internal requirement"
```

Controles que oferecem suporte a parâmetros personalizados

Para obter uma lista de controles de segurança que ofereçam suporte a parâmetros personalizados, consulte a página Controles no console do Security Hub ou a Referência de controles do Security Hub. Para recuperar essa lista programaticamente, é possível usar a operação ListSecurityControlDefinitions. Na resposta, o objeto `CustomizableProperties` indica quais controles oferecem suporte a parâmetros personalizáveis.

Controles do Security Hub que podem ser desabilitados

Recomendamos desativar alguns AWS Security Hub controles para reduzir o ruído de localização e limitar os custos.

Controles que lidam com recursos globais

Alguns Serviços da AWS oferecem suporte a recursos globais, o que significa que você pode acessar o recurso de qualquer um Região da AWS. Para economizar no custo de AWS Config, você pode desativar o registro de recursos globais em todas as regiões, exceto em uma. Depois de fazer isso, contudo, o Security Huib ainda executará verificações de segurança em todas as regiões em que os controles estejam habilitados e fará a cobrança com base no número de verificações por conta por região. Assim, para reduzir o ruído de localização e economizar no custo do Security Hub, você também deve desativar os controles que envolvem recursos globais em todas as regiões, exceto na região que registra os recursos globais.

Se um controle envolver recursos globais, mas estiver disponível em apenas uma região, desativá-lo nessa região impedirá que você obtenha quaisquer descobertas sobre o recurso subjacente. Nesse caso, recomendamos manter o controle ativado. Ao usar a agregação entre regiões, a região na qual o controle está disponível deve ser a região de agregação ou uma das regiões vinculadas. Os controles a seguir envolvem recursos globais, mas estão disponíveis somente em uma única região:

- Todos os CloudFront controles — Disponível somente no Leste dos EUA (Norte da Virgínia)
- GlobalAccelerator.1 — Disponível somente no Oeste dos EUA (Oregon)
- Route53.2 — Disponível somente no Leste dos EUA (Norte da Virgínia)
- WAF.1, WAF.6, WAF.7 e WAF.8 — Disponível somente no Leste dos EUA (Norte da Virgínia)

> **Note**
>
> Se você usar a configuração central, o Security Hub desativará automaticamente os controles que envolvem recursos globais em todas as regiões, exceto na região de origem. Outros controles que você escolhe ativar por meio de uma política de configuração são habilitados em todas as regiões em que estão disponíveis. Para limitar as descobertas desses controles a apenas uma região, você pode atualizar as configurações do AWS Config gravador e desativar a gravação global de recursos em todas as regiões, exceto na região de origem. Ao usar a configuração central, você não tem cobertura para um controle que não está disponível na região de origem e em nenhuma das regiões vinculadas. Para obter mais informações sobre a configuração central, consulte Como a configuração central funciona.

Se você desativar o registro de recursos globais em uma ou mais regiões, o controle [Config.1] que AWS Config deve ser ativado gera uma falha na descoberta nessas regiões. Isso ocorre porque o 2.5 requer o registro de recursos globais para ser aprovado. É possível suprimir as descobertas desse controle manualmente ou por meio de uma regra de automação.

Para controles com um tipo de programação periódico, é necessário desativá-los no Security Hub para evitar o faturamento. Definir o AWS Config parâmetro como `includeGlobalResourceTypes` `false` não afeta os controles periódicos do Security Hub.

Veja a seguir uma lista dos controles do Security Hub que envolvem recursos globais:

- [Conta.1] As informações de contato de segurança devem ser fornecidas para um Conta da AWS
- [A conta.2] Contas da AWS deve fazer parte de uma organização AWS Organizations
- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado

- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.1] As políticas do não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do não devem ter políticas do IAM anexadas
- [IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos
- [IAM.4] A chave de acesso do usuário raiz do não deve existir
- [IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- [IAM.7] As políticas de senha para usuários do IAM devem ter configurações fortes
- As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- [IAM.10] As políticas de senha para usuários do IAM devem ter durações fortes AWS Config
- 1.5 Certifique-se de que política de senha do IAM exija pelo menos uma letra maiúscula
- 1.6 Certifique-se de que política de senha do IAM exija pelo menos uma letra minúscula
- 1.7 Certifique-se de que política de senha do IAM exija pelo menos um símbolo
- Certifique-se de que política de senha do IAM exija pelo menos um número
- 1.9 Certifique-se de que a política de senha do IAM exija um comprimento mínimo de 14 ou mais
- 1.10 Certifique-se de que a política de senha do IAM impeça a reutilização de senhas
- 1.11 Certifique-se de que a política de senha do IAM expire senhas em até 90 dias ou menos
- [IAM.18] Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support

- [PCI.IAM.6] A MFA deve estar habilitada para todos os usuários do
- As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- As credenciais de usuário do IAM não utilizadas devem ser removidas
- As credenciais de usuário do IAM não utilizadas devem ser removidas
- As credenciais de usuário do IAM não utilizadas devem ser removidas
- As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras
- [WAF.10] as ACLs AWS WAF da web devem ter pelo menos uma regra ou grupo de regras
- [WAF.11] O registro de ACL AWS WAF da web deve estar ativado

Controles que lidam com o CloudTrail registro

Esse controle trata do uso de AWS Key Management Service (AWS KMS) para criptografar registros de AWS CloudTrail trilhas. Se você registrar essas trilhas em uma conta de registro centralizada, só precisará executar esses controles na conta e na região em que o registro centralizado ocorre.

> **Note**
>
> Se você usar a configuração central, o status de habilitação de um controle será alinhado entre a região inicial e as regiões vinculadas. Você não pode desabilitar um controle em algumas regiões e habilitá-lo em outras. Nesse caso, suprima as descobertas dos controles a seguir para reduzir o ruído de localização.

- [CloudTrail.2] CloudTrail deve ter a criptografia em repouso ativada

Controles que lidam com CloudWatch alarmes

Se você preferir usar a Amazon GuardDuty para detecção de anomalias em vez dos CloudWatch alarmes da Amazon, você pode desativar esses controles, que se CloudWatch concentram nos alarmes.

- [CloudWatch.1] Um filtro métrico de log e um alarme devem existir para uso do usuário “root”
- [CloudWatch.2] Certifique-se de que exista um filtro métrico de registro e um alarme para chamadas de API não autorizadas
- [CloudWatch.3] Certifique-se de que exista um filtro métrico de registro e um alarme para o login do Management Console sem MFA
- [CloudWatch.4] Certifique-se de que exista um filtro de métrica de log e um alarme para alterações na política do IAM
- [CloudWatch.5] Certifique-se de que exista um filtro métrico de log e um alarme para alterações de CloudTrail AWS Config duração
- [CloudWatch.6] Certifique-se de que exista um filtro métrico de registro e um alarme para falhas de AWS Management Console autenticação
- [CloudWatch.7] Certifique-se de que exista um filtro métrico de registro e um alarme para desativar ou excluir programadamente as chaves gerenciadas pelo cliente
- [CloudWatch.8] Certifique-se de que exista um filtro métrico de log e um alarme para alterações na política do bucket do S3
- [CloudWatch.9] Certifique-se de que exista um filtro métrico de registro e um alarme para alterações AWS Config de configuração
- [CloudWatch.10] Certifique-se de que exista um filtro métrico de log e um alarme para alterações no grupo de segurança
- [CloudWatch.11] Certifique-se de que exista um filtro métrico de registro e um alarme para alterações nas listas de controle de acesso à rede (NACL)
- [CloudWatch.12] Certifique-se de que exista um filtro métrico de log e um alarme para alterações nos gateways de rede
- [CloudWatch.13] Certifique-se de que exista um filtro métrico de log e um alarme para alterações na tabela de rotas

- [CloudWatch.14] Certifique-se de que exista um filtro métrico de log e um alarme para alterações de VPC

Visualizar detalhes de controles

Para cada AWS Security Hub controle, você pode exibir uma página com detalhes úteis.

A parte superior da página de detalhes do controle fornece uma visão geral do controle, incluindo:

- Status de habilitação — A parte superior da página informa se o controle está habilitado para pelo menos um padrão em pelo menos uma conta-membro. Se você tiver definido uma região de agregação, o controle será ativado se estiver habilitado para pelo menos um padrão em pelo menos uma região. Se o controle estiver desabilitado, será possível habilitá-lo nesta página. Se o controle estiver habilitado, será possível desabilitá-lo nesta página. Para ter mais informações, consulte the section called “Ativando e desativando controles no padrão”.
- Status do controle — Esse status resume o desempenho de um controle com base no status de conformidade das descobertas do controle. Normalmente, o Security Hub gera o status inicial do controle dentro de 30 minutos após sua primeira visita à página Resumo ou à página Padrões de segurança no console do Security Hub. Os status só estão disponíveis para controles que são ativados quando você visita essas páginas. Para habilitar ou desabilitar um controle programaticamente, use a operação da API do . Além disso, a gravação de AWS Config recursos deve ser configurada para que o status do controle apareça. Depois que os status de controle são gerados pela primeira vez, o Security Hub atualiza o status do controle a cada 24 horas com base nas descobertas das 24 horas anteriores. Na página de detalhes padrão e na página de detalhes do controle, o Security Hub exibe um timestamp para indicar quando o status foi atualizado pela última vez.

  Para contas de administrador, o status de controle reflete o status agregado da conta do administrador e de todas as contas dos membros. Se você definiu uma região de agregação, o status do controle inclui descobertas em todas as regiões vinculadas. Para obter mais informações sobre tabelas de controle, consulte the section called “Status de conformidade e status de controle”.

> **Note**
>
> Pode levar até 24 horas após a ativação de um controle para que os primeiros status de controle sejam gerados nas regiões da China e AWS GovCloud (US) Region.

A guia Padrões e requisitos lista os padrões para os quais um controle pode ser habilitado e os requisitos relacionados ao controle de diferentes estruturas de conformidade.

A parte inferior da página de detalhes contém informações sobre as descobertas ativas do controle. As descobertas de controle são geradas por verificações de segurança contra o controle. A lista de descobertas de controle não inclui descobertas arquivadas.

A lista de descoberta usa guias que exibem diferentes subconjuntos da lista. Na maioria das guias, a lista de descobertas mostra descobertas que têm um status de fluxo de trabalho de `NEW`, `NOTIFIED` ou `RESOLVED`. Uma guia separada exibe as descobertas `SUPPRESSED`.

Para cada descoberta, a lista fornece acesso aos detalhes da descoberta, como o status de conformidade e os recursos relacionados. Você também pode definir o status do fluxo de trabalho de cada descoberta e enviar as descobertas para ações personalizadas. Para ter mais informações, consulte the section called “Visualizar e executar ações em relação às descobertas”.

Visualizar detalhes de controles

Escolha seu método de acesso preferido e siga estas etapas para ver os detalhes de um controle. Os detalhes se aplicam à conta e região atuais e incluem o seguinte:

- Título e descrição do controle
- Link para instruções de correção para descobertas de controle malsucedidas
- Severidade do controle
- Status de habilitação do controle
- (No console) Uma lista das descobertas recentes do controle. Ao usar a API do Security Hub ou AWS CLI, use `GetFindings`para recuperar descobertas de controle.

Security Hub console

1. Abra o AWS Security Hub console em https://console.aws.amazon.com/securityhub/.

2. No painel de navegação, selecione Executar comando.
3. Selecione um controle.

Security Hub API

1. Execute o comando `ListSecurityControlDefinitions` e forneça um ou mais ARNs padrão para obter uma lista de IDs de controle. Para obter o ARN padrão, execute `DescribeStandards`. Se você não fornecer um ARN padrão, essa API retornará todas as IDs de controle do Security Hub. Essa API retorna IDs de controle de segurança independentes do padrão, não os IDs de controle baseados em padrão que existiam antes desses lançamentos de atributos.

   Exemplo de solicitação

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. Execute `BatchGetSecurityControls` para obter detalhes sobre um ou mais controles no atual Conta da AWS Região da AWS e.

   Exemplo de solicitação

   ```
   {
       "SecurityControlIds": ["Config.1", "IAM.1"]
   }
   ```

AWS CLI

1. Execute o comando `list-security-control-definitions` e forneça um ou mais ARNs padrão para obter uma lista de IDs de controle. Para obter o ARN padrão, execute `describe-standards`. Se você não fornecer um ARN padrão, essa API retornará todas as IDs de controle do Security Hub. Essa API retorna IDs de controle de segurança independentes do padrão, não os IDs de controle baseados em padrão que existiam antes desses lançamentos de atributos.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Execute batch-get-security-controls para obter detalhes sobre um ou mais controles na Conta da AWS e Região da AWS atuais.

```
aws securityhub --region us-east-1 batch-get-security-controls --security-
control-ids '["Config.1", "IAM.1"]'
```

Filtrar a lista de controles

Na página Controles, é possível ver uma lista dos seus controles. É possível filtrar e classificar a lista para se concentrar em um subconjunto específico de controles.

- Tudo ativado (controles que estão habilitados em pelo menos um padrão habilitado)
- Falha (controles com um status `Failed`)
- Desconhecido (controles com um status `Unknown`)
- Falha (controles com um status `Passed`)
- Desativado (controles que estão desativados em todos os padrões)
- Sem dados (controles sem descobertas)
- Todos (todos os controles, ativados e desativados, sem levar em conta o status do controle ou a contagem de descobertas)

Para obter mais informações sobre tabelas de controle, consulte Status de conformidade e status de controle.

Se você estiver usando a integração AWS Organizations e estiver conectado à conta de AWS Security Hub administrador, a guia Tudo ativado inclui controles que estão habilitados em pelo menos uma conta de membro. Se você definiu uma região de agregação, a guia Tudo ativado inclui controles que estão habilitados em pelo menos uma região vinculada.

A guia Conectar-se é exibida por padrão. Em cada guia, os controles são, por padrão, classificados por severidade, de Crítica a Baixa. Você também pode classificar os controles por ID de controle,

status de conformidade, severidade ou número de verificações malsucedidas. A barra de pesquisa permite que você pesquise controles específicos.

> **Tip**
>
> Se você tiver fluxos de trabalho automatizados com base em descobertas de controle, recomendamos usar os campos do ASFF `SecurityControlId` ou `SecurityControlArn` como filtros, em vez de `Title` ou `Description`. Os últimos campos podem mudar ocasionalmente, enquanto o ID de controle e o ARN são identificadores estáticos.

Escolher a opção ao lado do controle exibe um painel lateral que exibe os padrões nos quais o controle está atualmente ativado. Você também pode ver os padrões nos quais o controle está atualmente desativado. Nesse painel, é possível desativar um controle desativando-o em todos os padrões. Para obter mais informações sobre como habilitar e desabilitar controles entre padrões, consulte Ativando e desativando controles no padrão. Para contas de administrador, as informações apresentadas no painel lateral refletem todas as contas dos membros.

Na API do Security Hub, execute `ListSecurityControlDefinitions` para recuperar uma lista de IDs de controle. Depois de ter os IDs de controle nos quais está interessado, execute `BatchGetSecurityControls`para obter dados sobre esse subconjunto de controles para o atual Conta da AWS e. Região da AWS

Visualizar e executar ações em relação às descobertas

A página de detalhes do controle exibe uma lista das descobertas ativas de um controle. A lista de descobertas de controle não inclui descobertas arquivadas.

A página de detalhes do controle oferece suporte para a agregação de descobertas. Se você definiu uma região de agregação, o status do controle e a lista de verificações de segurança na página de detalhes do controle incluem verificações de todas as Regiões da AWS vinculadas.

A lista fornece ferramentas para filtrar e classificar as descobertas, para que você possa se concentrar primeiro nas descobertas mais urgentes. Uma descoberta pode incluir links para detalhes do recurso no console de serviço relacionado. Para controles baseados em AWS Config regras, você pode ver detalhes sobre a regra e o cronograma de configuração.

Você também pode usar a AWS Security Hub API para recuperar uma lista de descobertas. Para ter mais informações, consulte the section called “Analisando os detalhes da descoberta”.

Tópicos

Visualizando detalhes sobre uma descoberta de controle e um recurso de busca

AWS Security Hub fornece os seguintes detalhes para cada descoberta de controle para ajudá-lo a investigá-la:

- Um histórico das alterações que os usuários fizeram na descoberta
- Um arquivo `.json` para a descoberta
- Informações sobre o recurso relacionado à descoberta
- A regra de configuração relacionada à descoberta
- Observações que os usuários adicionaram à descoberta

A seção a seguir explica como acessar esses detalhes.

Histórico de descobertas

O histórico de descobertas é um recurso do Security Hub que permite rastrear as alterações feitas em uma descoberta nos últimos 90 dias.

O histórico de descobertas está disponível para descobertas de controle e outras descobertas do Security Hub. Para ter mais informações, consulte Analisando o histórico de descobertas.

Visualizar o arquivo.json completo para uma descoberta

É possível exibir e baixar o `.json` integral de uma descoberta.

Para exibir o `.json`, na coluna .json da descoberta, escolha o ícone.

No painel JSON da descoberta, para baixar o `.json`, escolha Baixar.

Visualizar informações sobre um recurso de descoberta

A coluna Recurso contém o tipo e o identificador do recurso.

Para exibir informações sobre o recurso, escolha o identificador do recurso. Na Contas da AWS, se a conta for uma conta-membro da organização, as informações incluirão o ID da conta e o nome da conta. Para as contas que são convidadas manualmente, as informações incluem apenas o ID da conta.

Se você tiver permissão para visualizar o recurso em seu serviço original, o identificador do recurso exibirá um link para o serviço. Por exemplo, para um AWS usuário, os detalhes do recurso fornecem um link para a visualização dos detalhes do usuário no IAM.

Se o recurso estiver em uma conta diferente, o Security Hub exibirá uma mensagem para notificá-lo.

Visualizando o cronograma de configuração de um recurso de descoberta

Uma via de investigação é o cronograma de configuração do recurso em AWS Config.

Se você tiver permissão para visualizar o cronograma de configuração do recurso de descoberta, a lista de descobertas fornecerá um link para o cronograma.

Se o recurso estiver em uma conta diferente, o Security Hub exibirá uma mensagem para notificá-lo.

Para navegar até a linha do tempo de configuração em AWS Config

1. Na coluna Investigar, escolha o ícone.
2. No menu, escolha Cronograma de configuração. Se você não tiver acesso ao cronograma de configuração, o link não será exibido.

Visualizando a AWS Config regra para um recurso de busca

Se o controle for baseado em uma AWS Config regra, talvez você também queira ver os detalhes da AWS Config regra. As informações da AWS Config regra podem ajudar você a entender melhor por que uma verificação foi aprovada ou falhou.

Se você tiver permissão para visualizar a AWS Config regra do controle, a lista de descobertas fornecerá um link para a AWS Config regra em AWS Config.

Se o recurso estiver em uma conta diferente, o Security Hub exibirá uma mensagem para notificá-lo.

Para navegar até a AWS Config regra

1. Na coluna Investigar, escolha o ícone.

2. No menu, escolha Configurar regra. Se você não tiver acesso à AWS Config regra, a regra Config não está vinculada.

Visualizar notas para descobertas

Se uma descoberta tiver uma nota associada, a coluna Atualizado exibirá um ícone de nota.

Para exibir a nota associada a uma descoberta

Na coluna Atualizado, escolha o ícone da nota.

Exemplo de descobertas de controle

O formato das descobertas de controle varia dependendo se você ativou as descobertas de controle consolidadas. Se você ativar as descobertas de controle consolidadas, o Security Hub gerará uma única descoberta para uma verificação de segurança, mesmo quando o controle estiver incluído em vários padrões habilitados. Para ter mais informações, consulte Ativar/desativar descobertas de controle consolidadas.

A seção a seguir mostra exemplos de descobertas de controle. Isso inclui descobertas de cada padrão do Security Hub quando as descobertas de controle consolidadas são desativadas em sua conta e uma amostra de descoberta de controle em todos os padrões quando ativadas.

> **Note**
>
> As descobertas farão referência a diferentes campos e valores nas regiões da China e AWS GovCloud (US) . Para ter mais informações, consulte Impacto da consolidação nos campos e valores do ASFF.

Ativar/desativar descobertas de controle consolidadas

- Exemplo de descoberta do padrão AWS Foundational Security Best Practices (FSBP)
- Exemplo de descoberta do Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0
- Exemplo de descoberta do Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0
- Exemplo de descoberta do Center for Internet Security (CIS) AWS Foundations Benchmark v3.0.0
- Instituto Nacional de Padrões e Tecnologia (National Institute of Standards and Technology, NIST) SP 800-53 (Revisão 4)

- Padrão de segurança de dados do setor de cartão de pagamento (PCI DSS – Payment Card Industry Data Security Standard)
- Exemplo de descoberta para o AWS Resource Tagging Standard
- Exemplo de descoberta do Service-Managed Standard: AWS Control Tower

Ativar/desativar descobertas de controle consolidadas

- Exemplo de descoberta em todos os padrões

Exemplo de descoberta para FSBP


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.076Z",
  "LastObservedAt": "2021-09-28T16:10:06.956Z",
  "CreatedAt": "2020-08-06T02:18:23.076Z",
  "UpdatedAt": "2021-09-28T16:10:00.093Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
```

```
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-
practices/v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/aws-foundation-best-practices/v/1.0.0"
    }]
  },
```

```
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
    ]
  }
}
```

Exemplo de descoberta para o CIS AWS Foundations Benchmark v3.0.0

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2024-04-18T07:46:18.193Z",
  "LastObservedAt": "2024-04-23T07:47:01.137Z",
  "CreatedAt": "2024-04-18T07:46:18.193Z",
  "UpdatedAt": "2024-04-23T07:46:46.165Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
```

```
  },
  "Title": "2.2.1 EBS default encryption should be enabled",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using
 the Elastic Block Store (EBS) service. While disabled by default, forcing encryption
 at EBS volume creation is supported.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/3.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0",
    "ControlId": "2.2.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2843ed9e",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v3.0.0/2.2.1"
```

```
    ],
    "SecurityControlId": "EC2.7",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  },
  "ProcessedAt": "2024-04-23T07:47:07.088Z"
}
```

Exemplo de descoberta para o CIS AWS Foundations Benchmark v1.4.0

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/1.4.0/3.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2022-10-21T22:14:48.913Z",
```

```
  "LastObservedAt": "2022-12-22T22:24:56.980Z",
  "CreatedAt": "2022-10-21T22:14:48.913Z",
  "UpdatedAt": "2022-12-22T22:24:52.409Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS CloudTrail is a web service that records AWS API calls for an
 account and makes those logs available to users and resources in accordance with IAM
 policies. AWS Key Management Service (KMS) is a managed service that helps create
 and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail logs
 can be configured to leverage server side encryption (SSE) and AWS KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0",
    "ControlId": "3.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-855f82d1",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/1.4.0/3.7",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
```

```
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  }
}
```

Exemplo de descoberta para o CIS AWS Foundations Benchmark v1.2.0

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/
rule/2.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
  ],
  "FirstObservedAt": "2020-08-29T04:10:06.337Z",
  "LastObservedAt": "2021-09-28T16:10:05.350Z",
  "CreatedAt": "2020-08-29T04:10:06.337Z",
  "UpdatedAt": "2021-09-28T16:10:00.087Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS Key Management Service (KMS) is a managed service that helps
 create and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail
 logs can be configured to leverage server side encryption (SSE) and KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsGuideArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0",
    "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0",
```

```
    "RuleId": "2.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/cis-aws-
foundations-benchmark/v/1.2.0/2.7",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
```

```
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ]
  }
}
```

Exemplo de descoberta para o NIST SP 800-53 Rev. 5

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-53/v/5.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2023-02-17T14:22:46.726Z",
  "LastObservedAt": "2023-02-17T14:22:50.846Z",
  "CreatedAt": "2023-02-17T14:22:46.726Z",
  "UpdatedAt": "2023-02-17T14:22:46.726Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to fix this issue, consult the AWS Security Hub
 NIST 800-53 R5 documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
```

```
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-53/v/5.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-53/v/5.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.9/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/
v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",

      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",

      "Partition": "aws",

      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
        "NIST.800-53.r5 AU-9",
        "NIST.800-53.r5 CA-9(1)",
        "NIST.800-53.r5 CM-3(6)",
        "NIST.800-53.r5 SC-13",
        "NIST.800-53.r5 SC-28",
        "NIST.800-53.r5 SC-28(1)",
        "NIST.800-53.r5 SC-7(10)",
        "NIST.800-53.r5 SI-7(6)"
    ],
    "SecurityControlId": "CloudTrail.2",
```

```
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-53/v/5.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2023-02-17T14:22:53.572Z"
}
```

Exemplo de descoberta para PCI DSS

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "pci-dss/v/3.2.1/PCI.CloudTrail.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.089Z",
  "LastObservedAt": "2021-09-28T16:10:06.942Z",
  "CreatedAt": "2020-08-06T02:18:23.089Z",
  "UpdatedAt": "2021-09-28T16:10:00.090Z",
  "Severity": {
```

```
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "PCI.CloudTrail.1 CloudTrail logs should be encrypted at rest using AWS KMS
 CMKs",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption by checking if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/pci-dss/v/3.2.1",
    "ControlId": "PCI.CloudTrail.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/pci-dss/
v/3.2.1/PCI.CloudTrail.1",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
```

```
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "PCI DSS 3.4"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/pci-dss/v/3.2.1"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
    ]
  }
}
```

Exemplo de descoberta para o AWS Resource Tagging Standard

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "security-control/EC2.44",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
```

```
  "FirstObservedAt": "2024-02-19T21:00:32.206Z",
  "LastObservedAt": "2024-04-29T13:01:57.861Z",
  "CreatedAt": "2024-02-19T21:00:32.206Z",
  "UpdatedAt": "2024-04-29T13:01:41.242Z",
  "Severity": {
    "Label": "LOW",
    "Normalized": 1,
    "Original": "LOW"
  },
  "Title": "EC2 subnets should be tagged",
  "Description": "This control checks whether an Amazon EC2 subnet has tags with the
 specific keys defined in the parameter requiredTagKeys. The control fails if the
 subnet doesn't have any tag keys or if it doesn't have all the keys specified in
 the parameter requiredTagKeys. If the parameter requiredTagKeys isn't provided, the
 control only checks for the existence of a tag key and fails if the subnet isn't
 tagged with any key. System tags, which are automatically applied and begin with aws:,
 are ignored.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.44/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-tagged-ec2-subnet-6ceafede",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "No tags are present.",
    "Resources:0/Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
    "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
securityhub/arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsEc2Subnet",
      "Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/subnet-1234567890abcdef0",
      "Partition": "aws",
      "Region": "eu-central-1",
      "Details": {
        "AwsEc2Subnet": {
```

```
          "AssignIpv6AddressOnCreation": false,
          "AvailabilityZone": "eu-central-1b",
          "AvailabilityZoneId": "euc1-az3",
          "AvailableIpAddressCount": 4091,
          "CidrBlock": "10.24.34.0/23",
          "DefaultForAz": true,
          "MapPublicIpOnLaunch": true,
          "OwnerId": "123456789012",
          "State": "available",
          "SubnetArn": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
          "SubnetId": "subnet-1234567890abcdef0",
          "VpcId": "vpc-021345abcdef6789"
        }
      }
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "EC2.44",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/aws-resource-tagging-standard/v/1.0.0"
      }
    ],
    "SecurityControlParameters": [
      {
        "Name": "requiredTagKeys",
        "Value": [
          "peepoo"
        ]
      }
    ],
            },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "LOW",
      "Original": "LOW"
    },
```

```
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2024-04-29T13:02:03.259Z"
}
```

Exemplo de descoberta do Service-Managed Standard: AWS Control Tower

> **Note**
>
> Esse padrão está disponível para você somente se você for um AWS Control Tower usuário que criou o padrão em AWS Control Tower. Para ter mais informações, consulte Padrão gerenciado por serviços: AWS Control Tower.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-
control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-11-17T01:25:30.296Z",
  "LastObservedAt": "2022-11-17T01:25:45.805Z",
  "CreatedAt": "2022-11-17T01:25:30.296Z",
  "UpdatedAt": "2022-11-17T01:25:30.296Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CT.CloudTrail.2 CloudTrail should have encryption at-rest enabled",
```

```
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/service-managed-aws-control-tower/
v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0",
    "ControlId": "CT.CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/service-
managed-aws-control-tower/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-
aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"
```

```
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}
```

Exemplo de descoberta em todos os padrões (quando as descobertas de controle consolidadas estão ativadas)

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "security-control/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-10-06T02:18:23.076Z",
  "LastObservedAt": "2022-10-28T16:10:06.956Z",
  "CreatedAt": "2022-10-06T02:18:23.076Z",
  "UpdatedAt": "2022-10-28T16:10:00.093Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": "40",
    "Original": "MEDIUM"
  },
```

```
  "Title": "CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
 the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
 key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  }
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
        "PCI DSS v3.2.1/3.4",
        "CIS AWS Foundations Benchmark v1.2.0/2.7",
        "CIS AWS Foundations Benchmark v1.4.0/3.7"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [
       { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
       { "StandardsId": "standards/pci-dss/v/3.2.1"},
       { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
```

```
        { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
        { "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
      ]
    },
    "WorkflowState": "NEW",
    "Workflow": {
      "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
      "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
      },
      "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards"
      ]
    }
}
```

Filtrar, classificar e baixar descobertas de controle

É possível filtrar a lista de descobertas de controle com base no status de conformidade usando as guias de filtragem. Você também pode filtrar a lista com base em outros valores do campo de descoberta e baixar as descobertas da lista.

Filtrar e classificar a lista de descobertas de controle

A guia Todas as verificações lista todas as descobertas ativas que têm um status de fluxo de trabalho de `NEW`, `NOTIFIED` ou `RESOLVED`. Por padrão, a guia Todos ativados é classificada de forma que os controles com falha estejam no topo da lista. Essa ordem de classificação ajuda você a priorizar as descobertas que precisam ser abordadas.

As listas nas guias Falha, Desconhecido e Aprovado são filtradas com base no valor de `Compliance.Status`. As contagens incluem apenas descobertas que têm um status de fluxo de trabalho de `NEW` ou .

A guia Suprimida contém uma lista de descobertas ativas que têm um status de fluxo de trabalho de `SUPPRESSED`.

Além dos filtros integrados em cada guia, é possível filtrar as listas usando valores dos seguintes campos:

- ID da conta
- Status do fluxo de trabalho
- Compliance status (Status de conformidade)
- ID do recurso
- Tipo de recurso

É possível classificar cada lista usando qualquer uma das colunas.

Baixar a lista de descobertas de controle

Se você navegar até Padrões de segurança e escolher um padrão, verá uma lista de controles para o padrão. A escolha de um controle na lista leva você à página de detalhes do controle com uma lista de descobertas do controle. A partir daqui, é possível baixar as descobertas de controle em um arquivo.csv.

Se você filtrou a lista de controles, o arquivo baixado incluirá somente os controles que correspondem às configurações do filtro.

Se você selecionar descobertas específicas na lista, o download incluirá somente as descobertas selecionadas.

Escolha Baixar agora para fazer download do arquivo. A página atual de descobertas é baixada.

Tomar medidas sobre as descobertas de controle

Para refletir o status atual da sua investigação, você define o status do fluxo de trabalho. Para ter mais informações, consulte the section called “Definir o status do fluxo de trabalho das descobertas”.

Em AWS Security Hub, você também pode enviar descobertas selecionadas para uma ação personalizada na Amazon EventBridge. Para ter mais informações, consulte the section called “Enviar descobertas para uma ação personalizada”.

Trabalho com o painel Resumo

No console do AWS Security Hub, o painel na página Resumo pode ajudá-lo a identificar áreas de preocupação com a segurança em seu ambiente da AWS, sem a necessidade de ferramentas de análise adicionais ou consultas complexas. É possível personalizar o layout do painel, adicionar ou remover widgets e filtrar os dados para se concentrar em áreas de interesse específico. Você também pode salvar seus critérios de filtro como um conjunto de filtros para recuperar rapidamente tipos de dados específicos no futuro.

Se você personalizar o painel ou filtrar os dados, o Security Hub salvará automaticamente suas configurações para uso posterior. Além disso, as configurações são salvas de forma independente para cada usuário da sua conta do Security Hub. Isso significa que usuários diferentes podem ter diferentes layouts, widgets e conjuntos de filtros para o painel.

Sempre que você abrir o painel Resumo, o Security Hub atualizará automaticamente a maioria dos dados do painel. Entretanto, alguns dos dados serão atualizados com menos frequência. Por exemplo, pontuações de segurança e status de controle são atualizados a cada 24 horas.

Se você configurou uma região de agregação entre regiões para o Security Hub, os dados do painel incluem descobertas da região de agregação e de todas as regiões vinculadas. Se você for o administrador delegado do Security Hub de uma organização, os dados incluem descobertas para sua conta de administrador e suas contas-membro. Opcionalmente, é possível filtrar os dados por conta. Se você tiver uma conta-membro ou uma conta independente, os dados incluem descobertas somente para sua conta.

Widgets disponíveis para o painel Resumo

O painel Resumo inclui widgets que refletem o cenário moderno de ameaças à segurança na nuvem, orientado pelas operações e experiências de segurança dos clientes da AWS. Alguns widgets são exibidos por padrão, ao passo que outros não. É possível personalizar sua visualização do painel adicionando ou removendo widgets.

Para adicioná-los, escolha Adicionar widget no canto superior direito da página Resumo. Na barra de pesquisa, insira o título do widget. Arraste e solte o widget no painel.

Widgets mostrados por padrão

Por padrão, o painel Resumo inclui os widgets a seguir:

Padrões de segurança

Exibe sua pontuação de segurança resumida mais recente e a pontuação de segurança de cada padrão do Security Hub. As pontuações de segurança, que variam de 0 a 100 por cento, representam a proporção de controles aprovados em relação a todos os controles habilitados. Para obter mais informações sobre essas pontuações, consulte Como as pontuações de segurança são calculadas. Esse widget ajuda você a entender sua postura geral de segurança.

Ativos com mais descobertas

Fornece uma visão geral dos recursos, contas e aplicações que têm mais descobertas. A lista é classificada em ordem decrescente pelo número de descobertas. No widget, cada guia mostra os seis principais itens dessa categoria, agrupados por gravidade e tipo de recurso. Se você escolher um número na coluna Total de descobertas, o Security Hub abrirá uma página que mostra as descobertas do ativo. Esse widget ajuda você a identificar rapidamente quais dos seus principais ativos apresentam possíveis ameaças à segurança.

Descobertas por região

Mostra o número total de descobertas, agrupadas por gravidade, em cada Região da AWS em que o Security Hub está habilitado. Esse widget ajuda você a identificar problemas de segurança que afetem potencialmente regiões específicas. Se você abrir o painel na sua região de agregação, esse widget ajudará você a monitorar possíveis problemas de segurança em cada região vinculada.

Tipos de ameaças mais comuns

Fornece um detalhamento dos 10 tipos mais comuns de ameaças em seu ambiente da AWS. Isso inclui ameaças como escalonamento de privilégios, uso de credenciais expostas ou comunicação com endereços IP maliciosos.

Para visualizar esses dados, o Amazon GuardDuty deve estar habilitado. Se estiver, escolha um tipo de ameaça nesse widget para abrir o console do GuardDuty e analisar as descobertas relacionadas a essa ameaça. Esse widget ajuda você a avaliar possíveis ameaças no contexto de outros problemas de segurança.

Vulnerabilidades de software com explorações

Fornece um resumo das vulnerabilidades de software que existem em seu ambiente da AWS e têm explorações conhecidas. Você também pode verificar uma análise das vulnerabilidades que têm e não têm correções disponíveis.

Para visualizar esses dados, o Amazon Inspector deve estar habilitado. Se estiver, escolha uma estatística neste widget para abrir o console do Amazon Inspector e analisar mais detalhes sobre a vulnerabilidade. Esse widget ajuda você a avaliar vulnerabilidades de software no contexto de outros problemas de segurança.

Novas descobertas ao longo do tempo

Mostra tendências no número de novas descobertas diárias nos últimos 90 dias. É possível dividir os dados por gravidade ou por provedor para obter contexto adicional. Esse widget ajuda você a entender se o volume de descobertas aumentou ou diminuiu em horários específicos nos últimos 90 dias.

Recursos com a maioria das descobertas

Fornece um resumo dos recursos que geraram a maioria das descobertas, detalhados pelos tipos de recursos a seguir: buckets do Amazon Simple Storage Service (Amazon S3), instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e funções do AWS Lambda.

No widget, cada guia se concentra em um dos tipos de recursos anteriores, listando as 10 instâncias de recursos que geraram mais descobertas. Para analisar as descobertas de um recurso específico, escolha a instância do recurso. Esse widget ajuda você a fazer a triagem das descobertas de segurança associadas a recursos comuns da AWS.

Widgets ocultos por padrão

Os widgets a seguir também estão disponíveis para o painel Resumo, mas estão ocultos por padrão:

AMIs com a maioria das descobertas

Fornece uma lista das 10 imagens de máquina da Amazon (AMI) que geraram a maioria das descobertas. Esses dados estarão disponíveis somente se o Amazon EC2 estiver habilitado para sua conta. Ele ajuda a identificar quais AMIs apresentam riscos potenciais de segurança.

Entidades principais do IAM com mais descobertas

Fornece uma lista dos 10 usuários do AWS Identity and Access Management (IAM) que geraram a maioria das descobertas. Esse widget ajuda a realizar tarefas administrativas e de cobrança. Ele mostra quais usuários contribuem mais para o uso do Security Hub.

Contas com o maior número de descobertas (por gravidade)

Mostra um gráfico das 10 contas que geraram mais descobertas, agrupadas por gravidade. Esse widget ajuda você a determinar em quais contas concentrar os esforços de análise e correção.

Contas com mais descobertas (por tipo de recurso)

Mostra um gráfico das 10 contas que geraram mais descobertas, agrupadas por tipo de recurso. Esse widget ajuda a determinar quais contas e tipos de recursos priorizar para análise e correção.

Insights

Lista cinco insights gerenciados pelo Security Hub e o número de descobertas que eles geraram. Os insights identificam uma área de segurança específica que requer atenção.

Últimas descobertas das integrações da AWS

Mostra o número de descobertas que você recebeu no Security Hub de Serviços da AWS integrados. Também mostra quando você recebeu as descobertas mais recentes de cada serviço integrado. Esse widget fornece dados consolidados de descobertas de vários Serviços da AWS. Para detalhar, escolha um serviço integrado. Em seguida, o Security Hub abrirá o console desse serviço.

Filtragem do painel Resumo

Para organizar dados no painel Resumo e incluir somente os dados de segurança mais relevantes para você, é possível filtrar o painel. Por exemplo, se você for membro de uma equipe de aplicações, poderá criar uma visualização dedicada para uma aplicação essencial em seu ambiente de produção. Se você for membro de uma equipe de segurança, poderá criar uma visualização dedicada que o ajude a se concentrar nas descobertas de alta gravidade. Para filtrar dados no painel Resumo, você insere os critérios de filtro na caixa de filtro acima do painel. Se você aplicar critérios de filtro, eles serão aplicados a todos os dados no painel, exceto aos dados nos widgets Insights e Padrões de segurança.

É possível filtrar os dados usando os campos a seguir:

- Nome da conta
- ID da conta
- Nome do recurso da Amazon (ARN) da aplicação
- Nome da aplicação
- Nome do produto (para um AWS service (Serviço da AWS) ou um produto de terceiros que envie descobertas ao Security Hub)
- Record state (Estado de registro)

- Região
- Recurso de tag
- Gravidade
- Status do fluxo de trabalho

Por padrão, os dados do painel são filtrados usando os critérios a seguir: `Workflow status` é `NOTIFIED` ou `NEW`, e `Record state` é `ACTIVE`. Esses critérios aparecem acima do painel, abaixo da caixa de filtro. Para remover esses critérios, escolha X no token de filtro para os critérios que você deseja remover.

Se você aplicar regras de filtros que queira usar novamente, poderá salvá-las como um conjunto de regras. Um conjunto de regras é um conjunto de critérios de filtro que você cria e salva para reaplicar ao analisar os dados no painel Resumo.

> **Note**
>
> Os campos a seguir não podem ser salvos como parte de um conjunto de filtros: ARN da aplicação, nome da aplicação e tag de recurso.

Criação e salvamento de conjuntos de filtros

Siga estas etapas para criar e salvar um conjunto de filtros.

Para criar e salvar um conjunto de filtros

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Resumo.
3. Na caixa de filtro acima do painel Resumo, insira os critérios de filtro para o conjunto de filtros.
4. No menu Limpar filtros, escolha Salvar novo conjunto de filtros.
5. Na caixa de diálogo Salvar conjunto de filtros, insira um nome para o conjunto de filtros.
6. (Opcional) Para usar o filtro definido por padrão sempre que você abrir a página Resumo, selecione a opção para defini-la como exibição padrão.
7. Escolha Save (Salvar).

Para alternar entre os conjuntos de filtros que você criou e salvou, use o menu Escolher um conjunto de filtros acima do painel Resumo. Quando você seleciona um conjunto de filtros, o Security Hub aplica os critérios do conjunto de filtros aos dados no painel.

Atualização ou exclusão de conjuntos de filtros

Siga estas etapas para atualizar ou excluir um conjunto de filtros existente. Se você excluir um conjunto de filtros atualmente definido como sua exibição padrão do painel Resumo, sua exibição padrão será redefinida para a exibição padrão do Security Hub.

Para atualizar ou excluir um conjunto de filtros

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Resumo.
3. No menu Escolher um conjunto de filtros, acima da página Resumo, escolha o conjunto de filtros.
4. No menu Limpar filtros, execute uma das ações a seguir:
   - Para atualizar o conjunto de filtros, escolha Atualizar conjunto de filtros atual. Em seguida, insira suas alterações na caixa de diálogo exibida.
   - Para excluir o conjunto de filtros, escolha Excluir conjunto de filtros atual. Em seguida, escolha Excluir na caixa de diálogo exibida.

Personalização do painel Resumo

É possível personalizar o painel Resumo de várias maneiras. É possível adicionar e remover widgets do painel. Também é possível reorganizar e redimensionar widgets no painel.

Se você personalizar o painel, o Security Hub aplicará suas alterações imediatamente e salvará as novas configurações do painel. Suas alterações serão aplicadas à sua exibição do painel em todas as Regiões da AWS e navegadores.

Para personalizar o painel Resumo

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Resumo.
3. Faça o seguinte:

- Para adicionar um widget, escolha Adicionar widgets no canto superior direito da página. Na barra de pesquisa, insira o título do widget a ser adicionado. Em seguida, arraste o widget até o local desejado.
- Para remover um widget, escolha os três pontos no canto superior direito do widget.
- Para mover um widget, escolha a alça no canto superior esquerdo do widget e, depois, arraste o widget para o local desejado.
- Para alterar o tamanho de um widget, escolha a alça de redimensionamento no canto inferior direito do widget. Arraste a borda do widget até que o widget tenha seu tamanho preferido.

Para restaurar posteriormente as configurações originais, escolha Redefinir o layout padrão na parte superior da página.

Criar recursos do Security Hub com AWS CloudFormation

AWS Security Hub integra-se com AWS CloudFormation, que é um serviço que ajuda você a modelar e configurar seus AWS recursos para que você possa gastar menos tempo criando e gerenciando seus recursos e infraestrutura. Você cria um modelo que descreve todos os AWS recursos que você deseja (como regras de automação) e AWS CloudFormation provisiona e configura esses recursos para você.

Ao usar AWS CloudFormation, você pode reutilizar seu modelo para configurar seus recursos do Security Hub de forma consistente e repetida. Descreva seus recursos uma vez e, em seguida, provisione os mesmos recursos repetidamente em várias Contas da AWS regiões.

Security Hub e AWS CloudFormation modelos

Para provisionar e configurar recursos para o Security Hub e serviços relacionados, você precisa entender como os modelos do AWS CloudFormation funcionam. Os modelos são arquivos de texto no formato JSON ou YAML. Esses modelos descrevem os recursos que você deseja provisionar em suas AWS CloudFormation pilhas.

Se você não estiver familiarizado com JSON ou YAML, você pode usar o AWS CloudFormation Designer para ajudá-lo a começar a usar modelos. AWS CloudFormation Para obter mais informações, consulte O que é AWS CloudFormation Designer? no Guia do AWS CloudFormation usuário.

Você pode criar AWS CloudFormation modelos para os seguintes tipos de recursos do Security Hub:

- Habilitar o Security Hub
- Designando o administrador delegado do Security Hub para uma organização
- Habilitar um padrão de segurança (API)
- Criação de uma visão personalizada
- Criar uma regra de automação
- Inscrever-se em uma integração de produtos de terceiros

Para obter mais informações, incluindo exemplos de modelos JSON e YAML para os recursos, consulte a Referência de tipo de recurso do AWS Security Hub no Guia do usuário do AWS CloudFormation .

Saiba mais sobre AWS CloudFormation

Para saber mais sobre isso AWS CloudFormation, consulte os seguintes recursos:

- AWS CloudFormation
- AWS CloudFormation Guia do usuário
- AWS CloudFormation API Reference
- AWS CloudFormation Guia do usuário da interface de linha de comando

Assinar os anúncios do Security Hub com o Amazon Simple Notification Service

Esta seção fornece informações sobre como se inscrever em anúncios do AWS Security Hub com o Amazon Simple Notification Service (Amazon SNS) para receber notificações sobre o Security Hub.

Depois de se inscrever, você receberá notificações sobre os seguintes eventos (anote o `AnnouncementType` correspondente para cada evento):

- `GENERAL` – Notificações gerais sobre o serviço Security Hub.
- `UPCOMING_STANDARDS_CONTROLS` – Os controles ou padrões específicos do Security Hub serão lançados em breve. Esse tipo de anúncio ajuda você a preparar fluxos de trabalho de resposta e remediação antes do lançamento.
- `NEW_REGIONS` – O suporte para o Security Hub está disponível em um novo Região da AWS.
- `NEW_STANDARDS_CONTROLS` – Novos controles ou padrões do Security Hub foram adicionados.
- `UPDATED_STANDARDS_CONTROLS` – Os controles ou padrões existentes do Security Hub foram atualizados.
- `RETIRED_STANDARDS_CONTROLS` – Os controles ou padrões existentes do Security Hub foram retirados.
- `UPDATED_ASFF` – A sintaxe, os campos ou os valores do AWS Formato do Security Finding (ASFF) foram atualizados.
- `NEW_INTEGRATION` – Novas integrações com outros serviços da AWS ou produtos de terceiros estão disponíveis.
- `NEW_FEATURE` – Novos atributos do Security Hub estão disponíveis.
- `UPDATED_FEATURE` – Os atributos existentes do Security Hub foram atualizados.

As notificações estão disponíveis em todos os formatos compatíveis com o Amazon SNS. Você pode assinar os anúncios do Security Hub em todas as áreas em que o Regiões da AWS Security Hub está disponível.

Um usuário deve ter permissões de `Subscribe` para se inscrever em um tópico do Amazon SNS. Você pode conseguir isso com as políticas do Amazon SNS, políticas do IAM ou ambas. Para obter mais informações, consulte Políticas do IAM e do Amazon SNS juntas no Guia do desenvolvedor do Amazon Simple Notification Service.

> **Note**
>
> O Security Hub envia anúncios do Amazon SNS sobre atualizações do serviço Security Hub para qualquer assinante Conta da AWS. Para receber notificações sobre as descobertas do Security Hub, consulte Gerenciando e revisando detalhes e histórico de busca.

Você pode se inscrever em uma fila do Amazon Simple Queue Service (Amazon SQS) para um tópico do Amazon SNS, mas deve usar o nome do recurso da Amazon (ARN) de tópico do Amazon SNS que esteja na mesma região. Para obter mais informações, consulte Tutorial: Inscrever-se em uma fila do Amazon SNS para um tópico do Amazon SQS no Guia do desenvolvedor do Amazon Simple Queue Service.

Você também pode usar uma função do AWS Lambda para invocar eventos quando receber notificações. Para obter mais informações, incluindo um exemplo de código de função, consulte Tutorial: Uso de AWS Lambda com o Amazon Simple Notification Service no Guia do desenvolvedor AWS Lambda.

Os ARNs de tópico do Amazon SNS para cada região são os seguintes.

Região da AWS	Tópico ARN do Amazon SNS
Leste dos EUA (Ohio)	`arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements`
Leste dos EUA (N. da Virgínia)	`arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements`
Oeste dos EUA (N. da Califórnia)	`arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements`
Oeste dos EUA (Oregon)	`arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`

Região da AWS	Tópico ARN do Amazon SNS
África (Cidade do Cabo)	`arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements`
Ásia-Pacífico (Hong Kong)	`arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements`
Ásia-Pacífico (Hyderabad)	`arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements`
Ásia-Pacífico (Jacarta)	`arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements`
Ásia-Pacífico (Mumbai)	`arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements`
Ásia-Pacífico (Osaka)	`arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements`
Ásia-Pacífico (Seul)	`arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements`
Ásia-Pacífico (Singapura)	`arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements`
Ásia-Pacífico (Sydney)	`arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements`

Região da AWS	Tópico ARN do Amazon SNS
Ásia-Pacífico (Tóquio)	`arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements`
Canadá (Central)	`arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements`
China (Pequim)	`arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements`
China (Ningxia)	`arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements`
Europe (Frankfurt)	`arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements`
Europa (Irlanda)	`arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements`
Europa (Londres)	`arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements`
Europa (Milão)	`arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements`
Europa (Paris)	`arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements`

Região da AWS	Tópico ARN do Amazon SNS
Europa (Espanha)	`arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements`
Europa (Estocolmo)	`arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements`
Europa (Zurique)	`arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements`
Israel (Tel Aviv)	`arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements`
Oriente Médio (Barém)	`arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements`
Oriente Médio (Emirados Árabes Unidos)	`arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements`
América do Sul (São Paulo)	`arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements`
AWS GovCloud (Leste dos EUA)	`arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements`
AWS GovCloud (Oeste dos EUA)	`arn:aws-us-gov:sns:us-gov-west-1:239334163374:SecurityHubAnnouncements`

Normalmente, as mensagens são as mesmas em todas as regiões de uma partição, então você pode se inscrever em uma região de cada partição para receber anúncios que afetam todas as regiões dessa partição. Os anúncios associados às contas de membro não são replicados na conta do administrador. Como resultado, cada conta, incluindo a conta de administrador, terá apenas uma cópia de cada anúncio. Você pode decidir qual conta deseja usar para assinar os anúncios do Security Hub.

Para obter informações sobre o custo da assinatura dos anúncios do Security Hub, consulte os preços do Amazon SNS.

Assinar os anúncios do Security Hub (console)

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Na lista de regiões, selecione a região da em que deseja se inscrever nos anúncios do Security Hub. Este exemplo usa a região `us-west-2`.
3. No painel de navegação, escolha Subscriptions (Assinaturas) e, em seguida, selecione Create subscription (Criar assinatura).
4. Insira o ARN do tópico na caixa com mesmo nome. Por exemplo, `arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`.
5. Em Protocolo, selecione como você deseja receber os anúncios do Security Hub. Se você escolher E-mail, em Endpoint, insira o endereço de e-mail que você deseja usar para receber anúncios.
6. Selecione Criar assinatura.
7. Confirmar a assinatura. Por exemplo, se você escolher o protocolo de e-mail, o Amazon SNS enviará uma mensagem de confirmação de assinatura ao e-mail que você forneceu.

Assinando os anúncios do Security Hub (AWS CLI)

1. Execute o seguinte comando:

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements --protocol email --notification-endpoint your_email@your_domain.com
```

2. Confirmar a assinatura. Por exemplo, se você escolher o protocolo de e-mail, o Amazon SNS enviará uma mensagem de confirmação de assinatura ao e-mail que você forneceu.

Formato de mensagem do Amazon SNS

Os exemplos a seguir mostram os anúncios do Security Hub do Amazon SNS sobre a introdução de novos controles de segurança. O conteúdo da mensagem varia de acordo com o tipo de anúncio, mas o formato é o mesmo para todos os tipos de anúncio. Opcionalmente, um campo `Link` que fornece detalhes sobre o anúncio pode ser incluído.

Exemplo: anúncio do Security Hub para novos controles (protocolo de e-mail)

```
{
"AnnouncementType":"NEW_STANDARDS_CONTROLS",
"Title":"[New Controls] 36 new Security Hub controls added to the AWS Foundational
 Security Best Practices standard",
"Description":"We have added 36 new controls to the AWS Foundational Security Best
 Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3,
 AutoScaling.4, AutoScaling.6), AWS CloudFormation (CloudFormation.1), Amazon
 CloudFront (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23,
 EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon
 Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12),
 Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes
 Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon
 Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3, NetworkFirewall.4,
 NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift
 (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
 (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
 Foundational Security Best Practices standard in an account and configured Security
 Hub to automatically enable new controls, these controls are enabled by default.
 Availability of controls can vary by Region. "
}
```

Exemplo: anúncio do Security Hub para novos controles (protocolo de e-mail JSON)

```
{
  "Type" : "Notification",
  "MessageId" : "d124c9cf-326a-5931-9263-92a92e7af49f",
  "TopicArn" : "arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements",
  "Message" : "{\"AnnouncementType\":\"NEW_STANDARDS_CONTROLS\",\"Title\":\"[New
 Controls] 36 new Security Hub controls added to the AWS Foundational Security Best
 Practices standard\",\"Description\":\"We have added 36 new controls to the AWS
 Foundational Security Best Practices standard. These include controls for Amazon
 Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), AWS CloudFormation
```

```
 (CloudFormation.1), Amazon CloudFront (CloudFront.10), Amazon Elastic Compute Cloud
 (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR)
 (ECR.1, ECR.2), Amazon Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5,
 ECS.8, ECS.10, ECS.12), Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon
 Elastic Kubernetes Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12,
 ELB.13, ELB.14), Amazon Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3,
 NetworkFirewall.4, NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7),
 Amazon Redshift (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
 (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
 Foundational Security Best Practices standard in an account and configured SSecurity
 Hub to automatically enable new controls, these controls are enabled by default.
 Availability of controls can vary by Region. \"}",
  "Timestamp" : "2022-08-04T19:11:12.652Z",
  "SignatureVersion" : "1",
  "Signature" :
 "HTHgNFRYMetCvisulgLM4CVySvK9qCXFPHQDxYl9tuCFQuIrd7YO4m4YFR28XKMgzqrF20YP
+EilipUm2SOTpEEtOTekU5bn74+YmNZfwr4aPFx0vUuQCVOshmHl37hjkiLjhCg/t53QQiLfP7MH
+MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUsOG8yiJVCBEJhJ1yS
+gkwJdhRk2UQab9RcAmE6COK3hRWcjDwqTXz5nR6Ywv1ZqZfLIl7gYKslt+jsyd/k+7kOqGmOJRDr7qhE7H
+7vaGRLOptsQnbW8VmeYnDbahEO8FV+Mp1rpV+7Qg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-56e67fcb41f6fec09b0196692625d385.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements:9d0230d7-d582-451d-9f15-0c32818bf61f"
}
```

Segurança no AWS Security Hub

A segurança na nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você contará com um datacenter e uma arquitetura de rede criados para atender aos requisitos das organizações com as maiores exigências de segurança.

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

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos compliance programsAWS. Para saber mais sobre os programas de conformidade que se aplicam ao AWS Security Hub, consulte AWS Services in Scope by Compliance Program.
- Segurança na nuvem: sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

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

Tópicos

Proteção de dados no AWS Security Hub

O modelo de responsabilidade compartilhada da AWS se aplica à proteção de dados no AWS Security Hub. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura

global que executa toda a 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 mais informações sobre a proteção de dados na Europa, consulte o artigo AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja asConta da AWS credenciais da e configure as contas de usuário individuais com o AWS IAM Identity Center ou o 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 [multi-factor authentication]) com cada conta.
- Use SSL/TLS para se comunicar com os atributos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure o registro em log das atividades da API e do usuário com o .AWS CloudTrail
- Use AWS as soluções de criptografia da , juntamente com todos os controles de segurança padrão dos 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 a AWS por meio de uma interface de linha de comandos ou uma API, use um endpoint do FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Name (Nome). Isso também é válido quando você trabalha com o Security Hub ou outro Serviços da AWS usando o console, a API, a AWS CLI, ou SDKs da AWS. 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.

Security Hub é um serviço que oferece vários locatários. Para garantir a proteção de dados, o Security Hub criptografa os dados em repouso e os dados em trânsito entre os serviços de componentes.

AWS Identity and Access Management para AWS Security Hub

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (fazer login) e autorizado (ter permissões) para usar recursos do Security Hub. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa o AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Security Hub.

Usuário do serviço: se você usa o serviço Security Hub para fazer seu trabalho, o administrador fornece as credenciais e as permissões necessárias. Para usar mais recursos do Security Hub para executar seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um recurso no Security Hub, consulte Solução de problemas de identidade e acesso do AWS Security Hub.

Administrador do serviço: se você for responsável pelos recursos do Security Hub na sua empresa, provavelmente terá acesso total ao Security Hub. Cabe a você determinar os atributos e recursos do

Security Hub que os usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como a empresa pode usar o IAM com o Security Hub, consulte Como AWS Security Hub funciona com o IAM.

Administrador do IAM: se você for um administrador do IAM, talvez queira saber detalhes sobre como é possível criar políticas para gerenciar o acesso ao Security Hub. Para visualizar exemplos de políticas baseadas em identidade do Security Hub que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade para o Security Hub.

Autenticando com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como uma identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia do usuário do AWS IAM Identity Center . Usar a autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário-raiz para tarefas diárias. Proteja as credenciais do usuário-raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte Tarefas que exigem credenciais de usuário-raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o . AWS IAM Identity Center Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte “What is IAM Identity Center?” (O que é o Centro de Identidade do IAM?) noAWS IAM Identity Center Guia do usuário do .

Grupos e usuários do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos depender de credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do usuário do IAM.

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

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

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte Usar perfis do IAM no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do usuário do IAM. Se você usar o IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões noAWS IAM Identity Center Guia do usuário do .
- Permissões temporárias para usuários do IAM: um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse 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 atributo para acesso entre contas, consulte Como os perfis do IAM diferem das políticas baseadas em atributo no Guia do usuário do IAM.

- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal de chamada, usando um perfil de serviço ou uma função vinculada ao serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Perfil de serviço: um perfil de serviço é um perfil do IAMhttps://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do usuário do IAM.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.
- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar 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 as funções do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciamento do acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a perfis, e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação, independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política

gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

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

Políticas baseadas em atributos são políticas em linha que estão localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

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

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

Outros tipos de política

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

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (perfil ou usuário do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade e dos seus limites de permissões. As políticas baseadas em atributo que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais

informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.

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

Vários tipos de política

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

Como AWS Security Hub funciona com o IAM

Antes de usar AWS Identity and Access Management para gerenciar o acesso ao Security Hub, saiba quais recursos do IAM estão disponíveis para uso com o Security Hub.

Atributos do IAM que você pode usar com o Amazon Macie

Atributo do IAM	Suporte do Macie
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não

Atributo do IAM	Suporte do Macie
Ações de políticas	Sim
atributos de políticas	Não
Chaves de condição de políticas	Sim
Listas de controle de acesso (ACLs)	Não
Controle de acesso por atributo (ABAC) – tags em políticas	Sim
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Sim

Para uma visão de alto nível de como o Security Hub e outros Serviços da AWS funcionam com a maioria dos recursos do IAM, veja Serviços da AWS como funciona com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para o Security Hub

É compatível com políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou atributos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas.

Não é possível especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou função à qual ela está anexado. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

O Security Hub oferece suporte a políticas baseadas em identidade. Para ter mais informações, consulte Exemplos de políticas baseadas em identidade para o Security Hub.

Políticas baseadas em recursos para o Security Hub

Oferece suporte a políticas baseadas em recursos	Não

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

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em atributo é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em atributo conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

O Security Hub não oferece suporte a políticas baseadas em recurso. Você não pode anexar uma política do IAM diretamente a um recurso do Security Hub.

Ações políticas para o Security Hub

Oferece suporte a ações de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

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

As ações de política no Security Hub usam o seguinte prefixo antes da ação:

```
securityhub:
```

Por exemplo, para conceder permissão a um usuário para ativar o Security Hub, que é uma ação que corresponde à `EnableSecurityHub` operação da API do Security Hub, inclua a `securityhub:EnableSecurityHub` ação em sua política. As instruções de política devem incluir um elemento `Action` ou `NotAction`. O Security Hub define seu próprio conjunto de ações que descreve as tarefas que você pode executar com esse serviço.

```
"Action": "securityhub:EnableSecurityHub"
```

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

```
"Action": [
      "securityhub:EnableSecurityHub",
      "securityhub:BatchEnableStandards"
```

Você também pode especificar várias ações usando curingas (*). Por exemplo, para especificar todas as ações que começam com a palavra `Get`, inclua a seguinte ação:

```
"Action": "securityhub:Get*"
```

No entanto, como prática recomendada, você deve criar políticas que sigam o princípio de privilégio mínimo. Em outras palavras, você deve criar políticas que incluem somente as permissões necessárias para executar uma tarefa específica.

O usuário deve ter acesso à `DescribeStandardsControl` operação para ter acesso a `BatchGetSecurityControlsBatchGetStandardsControlAssociations`, `ListStandardsControlAssociations` e.

O usuário deve ter acesso à `UpdateStandardsControls` operação para ter acesso `BatchUpdateStandardsControlAssociations` a `UpdateSecurityControl` e.

Para obter uma lista das ações do Security Hub, consulte Ações definidas por AWS Security Hub na Referência de Autorização de Serviço. Para obter exemplos de políticas que especificam ações do Security Hub, consulteExemplos de políticas baseadas em identidade para o Security Hub.

Recursos

Oferece suporte a atributos de políticas	Não

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

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

Para ações não compatíveis com permissões no nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

O Security Hub define os seguintes tipos de recursos:

- Hub
- Produto

- Agregador de localização, também conhecido como agregador entre regiões
- Regra de automação
- Política de configuração

Nas políticas, especifique os esses tipos de recursos usando os ARNs.

Para obter uma lista dos tipos de recursos do Security Hub e a sintaxe do ARN de cada um, consulte Tipos de recursos definidos por AWS Security Hub na Referência de Autorização de Serviço. Para saber quais ações você pode especificar para cada tipo de recurso, consulte Ações definidas por AWS Security Hub na Referência de Autorização de Serviço. Para obter exemplos de políticas que especificam os recursos, consulte Exemplos de políticas baseadas em identidade para o Security Hub.

Chaves de condição de política para o Security Hub

Compatível com chaves de condição de política específicas do serviço	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual principal pode executar ações em quais recursos, e em que condições.

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

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

Você também pode usar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos de política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para obter uma lista das chaves de condição do Security Hub, consulte Chaves de condição AWS Security Hub na Referência de Autorização de Serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas por AWS Security Hub. Para obter exemplos de políticas que usam chaves de condição, consulte Exemplos de políticas baseadas em identidade para o Security Hub.

Listas de controle de acesso (ACLs) no Security Hub

Oferece suporte a ACLs	Não

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

O Security Hub não oferece suporte a ACLs, o que significa que você não pode anexar uma ACL a um recurso do Security Hub.

Controle de acesso baseado em atributos (ABAC) com Security Hub

Oferece suporte a ABAC (tags em políticas)	Sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do atributo que ela está tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

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

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

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

Você pode anexar tags aos recursos do Security Hub. Você também pode controlar o acesso aos recursos fornecendo informações de tag no `Condition` elemento de uma política.

Para obter informações sobre a marcação de recursos do Security Hub, consulteMarcar recursos do AWS Security Hub. Para obter um exemplo de uma política baseada em identidade que controla o acesso a um recurso com base em tags, consulte Exemplos de políticas baseadas em identidade para o Security Hub.

Usar credenciais de segurança temporárias com o Security Hub

Oferece suporte a credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS “Trabalhe com o IAM” no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar perfis, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere

credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte Credenciais de segurança temporárias no IAM.

É possível usar credenciais temporárias para fazer login com federação, assumir um perfil do IAM ou assumir um perfil entre contas. Você obtém credenciais de segurança temporárias chamando operações de AWS STS API, como AssumeRoleou GetFederationToken.

O Security Hub suporta o uso de credenciais temporárias.

Sessões de acesso direto para o Security Hub

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

Por exemplo, o Security Hub faz solicitações de FAS para downstream Serviços da AWS quando você integra o Security Hub com AWS Organizations e quando designa a conta delegada de administrador do Security Hub para uma organização em Organizations.

Para outras tarefas, o Security Hub usa uma função vinculada ao serviço para realizar ações em seu nome. Para obter detalhes sobre esse perfil, consulte Funções vinculadas ao serviço para o Security Hub.

Funções de serviço para o Security Hub

O Security Hub não assume nem usa funções de serviço. Para realizar ações em seu nome, o Security Hub usa uma função vinculada ao serviço. Para obter detalhes sobre esse perfil, consulte Funções vinculadas ao serviço para o Security Hub.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode criar problemas operacionais com o uso do Security Hub. Edite as funções de serviço somente quando o Security Hub fornecer orientação para fazer isso.

Funções vinculadas ao serviço para o Security Hub

Oferece suporte a perfis vinculados ao serviço	Sim

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

O Security Hub usa uma função vinculada ao serviço para realizar ações em seu nome. Para obter detalhes sobre esse perfil, consulte Funções vinculadas ao serviço para o Security Hub.

Exemplos de políticas baseadas em identidade para o Security Hub

Por padrão, usuários e perfis não têm permissão para criar ou modificar recursos do Security Hub. Eles também não podem executar tarefas usando o AWS Management Console, a AWS CLI ou uma API da AWS. Um administrador deve criar as políticas do IAM que concedam aos usuários e aos perfis permissões para executar operações de API específicas nos recursos especificados que precisam. O administrador deve anexar essas políticas aos usuários ou grupos que exigem essas permissões.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documentos de política JSON, consulte Criar políticas na guia JSON no Guia do usuário do IAM.

Tópicos

- Práticas recomendadas de políticas
- Usar o console do Security Hub
- Exemplo: permitir que os usuários visualizem suas próprias permissões
- Exemplo: permitir que os usuários criem e gerenciem uma política de configuração

- Exemplo: permitir que os usuários visualizem as descobertas
- Exemplo: permitir que os usuários criem e gerenciem regras de automação

Práticas recomendadas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Security Hub em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com AWS as políticas gerenciadas pela e avance para as permissões de privilégio mínimo: para começar a conceder permissões a seus usuários e workloads, use as AWS políticas gerenciadas pela que concedem permissões para muitos casos de uso comuns. Elas estão disponíveis na sua Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. É possível também usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um AWS service (Serviço da AWS) específico, como o AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: Condição no Manual do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 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 houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir MFA

quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte 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 Security Hub

Para acessar o console do AWS Security Hub, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes dos recursos do Security Hub na 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.

Não é necessário conceder permissões mínimas do console para usuários que fazem chamadas somente à AWS CLI ou à AWS API. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Para garantir que esses usuários e funções possam usar o console do Security Hub, anexe também a seguinte política AWS gerenciada à entidade. Para obter mais informações, consulte Adicionar permissões a um usuário no Guia do usuário do IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
```

```
    ]
}
```

Exemplo: permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como é possível criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou de forma programática usando a AWS CLI ou a AWS API.

```
{
    "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": "*"
        }
    ]
}
```

Exemplo: permitir que os usuários criem e gerenciem uma política de configuração

Este exemplo mostra como você pode criar uma política do IAM que permita ao usuário criar, visualizar, atualizar e excluir políticas de configuração. Esse exemplo de política também permite que o usuário inicie, interrompa e visualize associações de políticas. Para que essa política do IAM funcione, o usuário deve ser o administrador delegado do Security Hub de uma organização.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateConfigurationPolicy",
                "securityhub:UpdateConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetConfigurationPolicy",
                "securityhub:ListConfigurationPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:DeleteConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetConfigurationPolicyAssociations",
                "securityhub:GetConfigurationPolicyAssociation",
                "securityhub:ListConfigurationPolicyAssociations"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "UpdateConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:StartConfigurationPolicyAssociation",
                "securityhub:StartConfigurationPolicyDisassociation"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemplo: permitir que os usuários visualizem as descobertas

Este exemplo mostra como você pode criar uma política do IAM que permita ao usuário visualizar as descobertas do Security Hub.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemplo: permitir que os usuários criem e gerenciem regras de automação

Este exemplo mostra como você pode criar uma política do IAM que permita que um usuário crie, visualize, atualize e exclua as regras de automação do Security Hub. Para que essa política do IAM funcione, o usuário deve ser administrador do Security Hub. Para limitar as permissões, por exemplo, para permitir que um usuário visualize apenas as regras de automação, você pode remover as permissões de criação, atualização e exclusão.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateAutomationRule",
                "securityhub:BatchUpdateAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetAutomationRules",
                "securityhub:ListAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchDeleteAutomationRules"
            ],
            "Resource": "*"
        }
    ]
}
```

Funções vinculadas ao serviço para o Security Hub

AWS Security Hubusa uma [função vinculada ao serviço AWS Identity and Access Management](#) (IAM) chamada. `AWSServiceRoleForSecurityHub` Essa função vinculada ao serviço é uma função do IAM vinculada diretamente ao Security Hub. É predefinido pelo Security Hub e inclui todas as permissões que o Security Hub exige para chamar outras pessoas Serviços da AWS e monitorar AWS recursos em seu nome. O Security Hub usa essa função vinculada ao serviço em todos os Regiões da AWS lugares em que o Security Hub está disponível.

Uma função vinculada ao serviço facilita a configuração do Security Hub, já que não é preciso adicionar as permissões necessárias manualmente. O Security Hub define as permissões da função vinculada ao serviço e, a menos que definido em contrário, somente o Security Hub pode assumir a função. As permissões definidas incluem a política de confiança e a política de permissões, a qual não pode ser anexada a nenhuma outra entidade do IAM.

Para ver os detalhes da função vinculada ao serviço, na página Configurações do console do Security Hub, escolha Geral e, em seguida, Exibir permissões do serviço.

Você poderá excluir a função vinculada ao serviço do Security Hub somente depois de desabilitá-lo em todas as regiões em que estiver habilitado. Isso protege seus recursos do Security Hub, porque não é possível remover inadvertidamente as permissões para acessá-los.

Para informações sobre outros serviços que são compatíveis com as funções vinculadas ao serviço, consulte Serviços AWS compatíveis com o IAM no Guia do usuário do IAM e procure pelos serviços com Sim na coluna Função vinculada ao serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Tópicos

- Permissões da função vinculada ao serviço do Security Hub
- Criar uma função vinculada ao serviço no Security Hub
- Editar uma função vinculada ao serviço no Security Hub
- Excluir uma função vinculada ao serviço no Security Hub

Permissões da função vinculada ao serviço do Security Hub

O Security Hub usa a função vinculada ao serviço chamada `AWSServiceRoleForSecurityHub`. É uma função vinculada ao serviço necessária do AWS Security Hub para acessar seus recursos. A função vinculada ao serviço permite que o Security Hub receba descobertas de outros Serviços da AWS e configure o requisito de infraestrutura do AWS Config necessário para executar verificações de segurança dos controles.

A função vinculada ao serviço `AWSServiceRoleForSecurityHub` confia nos seguintes serviços para aceitar a função:

- `securityhub.amazonaws.com`

A função vinculada ao serviço AWSServiceRoleForSecurityHub usa a política gerenciada AWSSecurityHubServiceRolePolicy.

É necessário conceder permissões para permitir que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para que a função vinculada ao serviço AWSServiceRoleForSecurityHub seja criada com êxito, a identidade do IAM usada por você para acessar o Security Hub ter as permissões necessárias. Para conceder as permissões necessárias, anexe a seguinte política ao usuário, grupo ou função do.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Criar uma função vinculada ao serviço no Security Hub

A função vinculada ao serviço AWSServiceRoleForSecurityHub é criada automaticamente quando você habilita o Security Hub pela primeira vez ou habilita o Security Hub em uma região compatível na qual ele não tenha sido habilitado anteriormente. Também é possível criar a função vinculada ao serviço AWSServiceRoleForSecurityHub manualmente usando o console do IAM, o IAM CLI ou o IAM API.

> **Important**
>
> A função vinculada ao serviço criada para a conta de administrador do Security Hub não se aplica às contas-membro do Security Hub.

Para mais informações sobre a criação da função manualmente, consulte Criar uma função vinculada ao serviço no Guia do usuário do IAM.

Editar uma função vinculada ao serviço no Security Hub

O Security Hub não permite que você edite a função vinculada a serviço `AWSServiceRoleForSecurityHub`. Depois que você criar um perfil vinculado ao serviço, não poderá alterar o nome do perfil, pois várias entidades podem fazer referência ao perfil. No entanto, será possível editar a descrição da função usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço no Security Hub

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não terá uma entidade não utilizada e não monitorada ativamente ou mantida.

> **Important**
>
> Para excluir a função vinculada ao serviço `AWSServiceRoleForSecurityHub`, primeiro desabilite o Security Hub em todas as regiões em que estiver habilitado.
> Se o Security Hub não estiver desabilitado quando você tentar excluir a função vinculada ao serviço, haverá falha na exclusão. Para ter mais informações, consulte Desabilitar o Security Hub.

Quando você desabilitar o Security Hub, a função vinculada ao serviço `AWSServiceRoleForSecurityHub` não será automaticamente excluída. Se você habilitar o Security Hub novamente, ele começará usando a função vinculada ao serviço `AWSServiceRoleForSecurityHub` existente.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console, a CLI ou a API do IAM para excluir a função vinculada ao serviço `AWSServiceRoleForSecurityHub`. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

AWS políticas gerenciadas para o AWS Security Hub

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) for lançada ou novas operações de API forem disponibilizadas para serviços existentes.

Para mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

AWS política gerenciada: AWSSecurityHubFullAccess

É possível anexar a política `AWSSecurityHubFullAccess` a suas identidades do IAM.

Essa política concede permissões administrativas que oferecem às entidades principais acesso total a todas as ações do Security Hub. Essa política deve ser anexada a uma entidade principal antes que ele habilite o Security Hub manualmente para sua conta. Por exemplo, entidades principais com essas permissões podem visualizar e atualizar o status das descobertas. Elas podem configurar insights personalizados e habilitar integrações. Também podem habilitar e desabilitar padrões e controles. As entidades principais de uma conta de administrador também podem gerenciar contas-membro.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `securityhub` – Permite que as entidades principais acessem totalmente todas as ações do Security Hub.
- `guardduty`— Permite que os diretores obtenham informações sobre o status da conta na Amazon GuardDuty.
- `iam` – Permite que as entidades principais criem uma função vinculada ao serviço.
- `inspector`: permite que as entidades principais obtenham informações sobre o status da conta no Amazon Inspector.
- `pricing`— Permite que os diretores obtenham uma lista de preços Serviços da AWS e produtos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecurityHubAllowAll",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Sid": "SecurityHubServiceLinkedRole",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        },
        {
            "Sid": "OtherServicePermission",
            "Effect": "Allow",
            "Action": [
                "guardduty:GetDetector",
                "guardduty:ListDetectors",
                "inspector2:BatchGetAccountStatus",
                "pricing:GetProducts"
            ],
            "Resource": "*",
        }
```

```
    ]
}
```

Política gerenciada do Security Hub: AWSSecurityHubReadOnlyAccess

É possível anexar a política `AWSSecurityHubReadOnlyAccess` a suas identidades do IAM.

Essa política concede permissões de acesso somente para leitura que permitem que os usuários visualizem informações no Security Hub. As entidades principais com esta política anexada não podem fazer nenhuma atualização no Security Hub. Por exemplo, entidades principais com essas permissões podem ver a lista de descobertas associadas à conta, mas não podem alterar o status de uma descoberta. Elas podem ver os resultados dos insights, mas não podem criar ou configurar insights personalizados. Também não podem configurar controles ou integrações de produtos.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `securityhub` – Permite que os usuários realizem ações que retornem uma lista de itens ou detalhes sobre um item. Isso inclui operações de API que começam com `Get`, `List` ou `Describe`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSSecurityHubReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "securityhub:Get*",
                "securityhub:List*",
                "securityhub:BatchGet*",
                "securityhub:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS política gerenciada: AWSSecurityHubOrganizationsAccess

É possível anexar a política `AWSSecurityHubOrganizationsAccess` a suas identidades do IAM.

Essa política concede permissões administrativas AWS Organizations que são necessárias para suportar a integração do Security Hub com Organizations.

Essas permissões permitem que a conta de gerenciamento da organização designe a conta de administrador delegado do Security Hub. A conta de administrador delegado do Security Hub pode habilitar outras contas da organização como sendo contas-membro.

Essa política fornece apenas as permissões para o Organizations. A conta de gerenciamento da organização e a conta de administrador delegado do Security Hub também exigem permissões para as ações associadas no Security Hub. Essas permissões podem ser concedidas usando a política gerenciada do `AWSSecurityHubFullAccess`.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `organizations:ListAccounts`: permite que as entidades principais recuperem a lista de contas que sejam parte de uma organização.
- `organizations:DescribeOrganization`: permite que as entidades principais recuperem informações sobre a organização.
- `organizations:ListRoots`: permite que as entidades principais listem a raiz de uma organização.
- `organizations:ListDelegatedAdministrators`: permite que as entidades principais listem o administrador delegado de uma organização.
- `organizations:ListAWSServiceAccessForOrganization`— Permite que os diretores listem o Serviços da AWS que uma organização usa.
- `organizations:ListOrganizationalUnitsForParent`: permite que as entidades principais listem as unidades organizacionais (OU) filha de uma OU pai.
- `organizations:ListAccountsForParent`: permite que as entidades principais listem as contas filhas de uma OU pai.
- `organizations:DescribeAccount`: permite que as entidades principais recuperem informações sobre uma conta na organização.

- `organizations:DescribeOrganizationalUnit`: permite que as entidades principais recuperem informações sobre uma OU na organização.
- `organizations:DescribeOrganization` – Permite que as entidades principais recuperem informações sobre a configuração da organização.
- `organizations:EnableAWSServiceAccess` – Permite que as entidades principais habilitem a integração do Security Hub com o Organizations.
- `organizations:RegisterDelegatedAdministrator` – Permite que as entidades principais designem a conta de administrador delegado do Security Hub.
- `organizations:DeregisterDelegatedAdministrator` – Permite que as entidades principais designem a conta de administrador delegado do Security Hub.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OrganizationPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:ListRoots",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAccountsForParent",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganizationalUnit"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationPermissionsEnable",
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "securityhub.amazonaws.com"
                }
            }
```

```
        },
        {
            "Sid": "OrganizationPermissionsDelegatedAdmin",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator"
            ],
            "Resource": "arn:aws:organizations::*:account/o-*/*",
            "Condition": {
            "StringEquals": {
                "organizations:ServicePrincipal": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

AWS política gerenciada: AWSSecurityHubServiceRolePolicy

Não é possível anexar `AWSSecurityHubServiceRolePolicy` às entidades do IAM. Essa política é anexada a uma função vinculada ao serviço que permite que o Security Hub realize ações em seu nome. Para ter mais informações, consulte the section called “Perfis vinculados ao serviço”.

Essa política concede permissões administrativas que permitem que a função vinculada ao serviço execute verificações de segurança dos controles do Security Hub.

Detalhes da permissão

Esta política inclui permissões para fazer o seguinte:

- `cloudtrail`— Recupere informações sobre CloudTrail trilhas.
- `cloudwatch`— Recupere os alarmes atuais CloudWatch .
- `logs`— Recupere os filtros métricos dos CloudWatch registros.
- `sns` – Recuperar a lista de assinaturas de um tópico do SNS.
- `config`— recupere informações sobre gravadores de configuração, recursos e AWS Config regras. Também permite que a função vinculada ao serviço crie e exclua regras do AWS Config e execute avaliações com base nas regras.
- `iam` – Obter e gerar relatórios de credenciais para contas.

- `organizations` – Recuperar as informações da conta e da unidade organizacional (OU) de uma organização.
- `securityhub` – Recuperar informações sobre como o serviço, os padrões e os controles do Security Hub estão configurados.
- `tag` – Recuperar informações sobre tags de recursos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SecurityHubServiceRolePermissions",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:GetEventSelectors",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeAlarmsForMetric",
                "logs:DescribeMetricFilters",
                "sns:ListSubscriptionsByTopic",
                "config:DescribeConfigurationRecorders",
                "config:DescribeConfigurationRecorderStatus",
                "config:DescribeConfigRules",
                "config:DescribeConfigRuleEvaluationStatus",
                "config:BatchGetResourceConfig",
                "config:SelectResourceConfig",
                "iam:GenerateCredentialReport",
                "organizations:ListAccounts",
                "config:PutEvaluations",
                "tag:GetResources",
                "iam:GetCredentialReport",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListChildren",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "securityhub:BatchDisableStandards",
                "securityhub:BatchEnableStandards",
                "securityhub:BatchUpdateStandardsControlAssociations",
                "securityhub:BatchGetSecurityControls",
                "securityhub:BatchGetStandardsControlAssociations",
```

```
                "securityhub:CreateMembers",
                "securityhub:DeleteMembers",
                "securityhub:DescribeHub",
                "securityhub:DescribeOrganizationConfiguration",
                "securityhub:DescribeStandards",
                "securityhub:DescribeStandardsControls",
                "securityhub:DisassociateFromAdministratorAccount",
                "securityhub:DisassociateMembers",
                "securityhub:DisableSecurityHub",
                "securityhub:EnableSecurityHub",
                "securityhub:GetEnabledStandards",
                "securityhub:ListStandardsControlAssociations",
                "securityhub:ListSecurityControlDefinitions",
                "securityhub:UpdateOrganizationConfiguration",
                "securityhub:UpdateSecurityControl",
                "securityhub:UpdateSecurityHubConfiguration",
                "securityhub:UpdateStandardsControl",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SecurityHubServiceRoleConfigPermissions",
            "Effect": "Allow",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:GetComplianceDetailsByConfigRule"
            ],
            "Resource": "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
        },
        {
            "Sid": "SecurityHubServiceRoleOrganizationsPermissions",
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "securityhub.amazonaws.com"
                    ]
                }
```

```
            }
        }
    ]
}
```

Atualizações do Security Hub para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Security Hub desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações realizadas nesta página, inscreva-se no feed RSS na página Histórico de documentos do Security Hub.

Alteração	Descrição	Data
AWSSecurityHubFullAccess— Atualização de uma política existente	O Security Hub atualizou a política para obter detalhes de preços Serviços da AWS e produtos.	24 de abril de 2024
AWSSecurityHubReadOnlyAccess— Atualização de uma política existente	O Security Hub atualizou essa política gerenciada adicionando um `Sid` campo.	22 de fevereiro de 2024
AWSSecurityHubFullAccess— Atualização de uma política existente	O Security Hub atualizou a política para determinar se a Amazon GuardDuty e o Amazon Inspector estão habilitados em uma conta. Isso ajuda os clientes a reunir informações relacionadas à segurança de várias. Serviços da AWS	16 de novembro de 2023
AWSSecurityHubOrganizationsAccess— Atualização de uma política existente	O Security Hub atualizou a política para conceder permissões adicionais para permitir acesso somente para	16 de novembro de 2023

Alteração	Descrição	Data
	leitura à funcionalidade do administrador delegado do AWS Organizations . Isso inclui detalhes como raiz, unidades organizacionais (OUs), contas, estrutura organizacional e acesso ao serviço.	
AWSSecurityHubServiceRolePolicy: atualização para uma política existente	O Security Hub adicionou as permissões `BatchGetSecurityControls` , `DisassociateFromAdministratorAccount` e `UpdateSecurityControl` e para ler e atualizar propriedades de controle de segurança personalizáveis.	26 de novembro de 2023
AWSSecurityHubServiceRolePolicy: atualização para uma política existente	O Security Hub adicionou a permissão `tag:GetResources` para ler tags de recursos relacionadas às descobertas.	7 de novembro de 2023
AWSSecurityHubServiceRolePolicy: atualização para uma política existente	O Security Hub adicionou a permissão `BatchGetStandardsControlAssociations` para obter informações sobre o status de habilitação de um controle em um padrão.	27 de setembro de 2023

Alteração	Descrição	Data
AWSSecurityHubServiceRolePolicy: atualização para uma política existente	O Security Hub adicionou novas permissões para obter AWS Organizations dados, ler e atualizar as configurações do Security Hub, incluindo padrões e controles.	20 de setembro de 2023
AWSSecurityHubServiceRolePolicy: atualização para uma política existente	O Security Hub moveu a permissão `config:DescribeConfigRuleEvaluationStatus` existente para uma declaração diferente dentro da política. A permissão `config:DescribeConfigRuleEvaluationStatus` agora é aplicada a todos os recursos.	17 de março de 2023
AWSSecurityHubServiceRolePolicy: atualização para uma política existente	O Security Hub moveu a permissão `config:PutEvaluations` existente para uma declaração diferente dentro da política. A permissão `config:PutEvaluations` agora é aplicada a todos os recursos.	14 de julho de 2021
AWSSecurityHubServiceRolePolicy: atualização para uma política existente	O Security Hub adicionou uma nova permissão para permitir que a função vinculada ao serviço forneça resultados de avaliação para o AWS Config.	29 de junho de 2021

Alteração	Descrição	Data
AWSSecurityHubServiceRolePolicy— Adicionado à lista de políticas gerenciadas	Foram adicionadas informações sobre a política gerenciada AWSSecurityHubServiceRolePolicy, que é usada pela função vinculada ao serviço do Security Hub.	11 de junho de 2021
AWSSecurityHubOrganizationsAccess— Nova política	O Security Hub adicionou uma nova política que concede as permissões necessárias para a integração do Security Hub com o Organizations.	15 de março de 2021
O Security Hub começou a monitorar alterações	O Security Hub começou a monitorar as mudanças em suas políticas AWS gerenciadas.	15 de março de 2021

Solução de problemas de identidade e acesso do AWS Security Hub

Use as seguintes informações para ajudar você a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o Security Hub e o IAM.

Tópicos

- Não tenho autorização para executar uma ação no Security Hub
- Não estou autorizado a realizar iam: PassRole
- Quero acesso programático ao Security Hub
- Sou administrador e quero permitir que outras pessoas tenham acesso ao Security Hub
- Quero permitir que as pessoas fora da minha Conta da AWS acessem meus recursos do Security Hub.

Não tenho autorização para executar uma ação no Security Hub

Se o AWS Management Console informar que você não está autorizado a executar uma ação, você deverá entrar em contato com o administrador para obter assistência. Seu administrador é a pessoa que forneceu a você suas credenciais de início de sessão.

O exemplo de erro a seguir ocorre quando o usuário `mateojackson` tenta usar o console para visualizar detalhes sobre um *`widget`*, mas não tem `securityhub:`*`GetWidget`*as permissões.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

Neste caso, Mateo pede ao administrador para atualizar suas políticas para permitir a ele o acesso ao recurso *`my-example-widget`* usando a ação `securityhub:`*`GetWidget`*.

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, suas políticas deverão ser atualizadas para permitir a passagem de um perfil para o Security Hub.

Alguns Serviços da AWS permitem que você passe um perfil existente para o serviço, em vez de criar um novo perfil de serviço ou perfil vinculado ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O erro de exemplo a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para executar uma ação no Security Hub. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se você precisar de ajuda, entre em contato com seu administrador AWS. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero acesso programático ao Security Hub

Os usuários precisam de acesso programático se quiserem interagir com a AWS de fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando a AWS.

Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

Qual usuário precisa de acesso programático?	Para	Por
Identificação da força de trabalho (Usuários gerenciados no Centro de Identidade do IAM)	Use credenciais temporárias para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS.	Siga as instruções da interface que deseja utilizar. • Para a AWS CLI, consulte Configuração da AWS CLI para usar o AWS IAM Identity Center no AWS Command Line Interface Guia do usuário da . • Para os SDKs da AWS, ferramentas e APIs da AWS, consulte Autenticação do Centro de Identidade do IAM no Guia de referência de ferramentas e SDKs da AWS.
IAM	Use credenciais temporárias para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS.	Siga as instruções em Como usar credenciais temporárias com recursos da AWS no Guia do usuário do IAM.
IAM	(Não recomendado) Use credenciais de longo prazo para assinar solicitaç ões programáticas para a	Siga as instruções da interface que deseja utilizar.

Qual usuário precisa de acesso programático?	Para	Por
	AWS CLI, os SDKs da AWS ou as APIs da AWS.	• Para a AWS CLI, consulte Autenticação usando as credenciais de usuário do IAM no Guia do usuário da AWS Command Line Interface. • Para as ferramentas e SDKs da AWS, consulte Autenticação usando as credenciais de longo prazo no Guia de referência de ferramentas e SDKs da AWS. • Para as APIs da AWS, consulte Gerenciamento de chaves de acesso de usuários do IAM no Guia do usuário do IAM.

Sou administrador e quero permitir que outras pessoas tenham acesso ao Security Hub

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

- Usuários e grupos no AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Create a permission set (Criação de um conjunto de permissões) no Guia do usuário do AWS IAM Identity Center.

- Usuários gerenciados no IAM com provedor de identidades:

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

- Usuários do IAM:

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

Quero permitir que as pessoas fora da minha Conta da AWS acessem meus recursos do Security Hub.

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir a função. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), é possível usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Security Hub é compatível com esses recursos, consulte Como AWS Security Hub funciona com o IAM.
- Para saber como conceder acesso a seus recursos em todas as Contas da AWS pertencentes a você, consulte Fornecer acesso a um usuário do IAM em outra Conta da AWS pertencente a você no Guia de usuário do IAM.
- Para saber como conceder acesso a seus recursos para terceiros Contas da AWS, consulte Fornecimento de acesso a Contas da AWS pertencentes a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em atributos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em atributos no Guia do usuário do IAM.

Validação de conformidade do AWS Security Hub

Auditores de terceiros avaliam a segurança e a conformidade do AWS Security Hub como parte de vários programas de conformidade da AWS. Isso inclui SOC, PCI, FedRAMP, HIPAA e outros.

Para obter uma lista dos produtos da AWS no escopo de programas de conformidade específicos, consulte Produtos da AWS no escopo por programa de conformidade. Para obter informações gerais, consulte Programas de conformidade da AWS.

Você pode baixar relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Baixar os relatórios no AWS Artifact.

Sua responsabilidade de conformidade ao usar o Security Hub é determinada pela confidencialidade 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 conformidade – Esses guias de implantação discutem considerações sobre arquitetura e fornecem medidas para implantar ambientes de linha de base focados em segurança e conformidade na AWS.
- Recursos de compatibilidade da AWS – Esta coleção de guias e pastas de trabalho pode ser aplicada ao seu setor e local.
- AWS Config: esse serviço da AWS avalia até que ponto suas configurações de recursos atendem adequadamente às práticas internas e às diretrizes e regulamentações do setor.
- AWS Security Hub: esse serviço da AWS fornece uma visão abrangente do estado da segurança na AWS que ajuda verificar a conformidade com os padrões e as práticas recomendadas de segurança do setor.

Resiliência no AWS Security Hub

A infraestrutura global da AWS é criada com base em Regiões da AWS e zonas de disponibilidade. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, alta throughput e redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

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

Segurança da infraestrutura no AWS Security Hub

Por ser um serviço gerenciado, o AWS Security Hub é protegido pela segurança da rede global da AWS. Para obter informações sobre AWS serviços de segurança da AWS e como a protege a infraestrutura, consulte AWSSegurança na Nuvem . Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança de infraestrutura, consulte Proteção de infraestrutura em Pilar de segurança: AWS Well-Architected Framework.

Você usa chamadas de API publicadas pela AWS para acessar o Security Hub por meio da rede. Os clientes precisam oferecer suporte para:

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

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

AWS Security Hub e VPC endpoints de interface (AWS PrivateLink)

É possível estabelecer uma conexão privada entre a VPC e o AWS Security Hub criando um VPC endpoint de interface. Os endpoints de interface são habilitados pelo AWS PrivateLink, uma tecnologia que permite acessar de forma privada as APIs do Security Hub sem um gateway da Internet, um dispositivo NAT, uma conexão VPN ou uma conexão do AWS Direct Connect. As instâncias na sua VPC não precisam de endereços IP públicos para a comunicação com APIs do Security Hub. O tráfego de rede entre a sua VPC e o Security Hub não sai da rede Amazon.

Cada endpoint de interface é representado por uma ou mais interfaces de rede elástica nas sub-redes.

Para mais informações, consulte Endpoints da VPC de interface(AWS PrivateLink) no Guia AWS PrivateLink.

Considerações sobre os endpoints da VPC do Security Hub

Antes de configurar um endpoint da VPC de interface para o Security Hub, revise as Propriedades e limitações de endpoints de interface no Guia AWS PrivateLink.

O Security Hub é compatível com chamadas para todas as ações de API da sua VPC.

> **Note**
>
> O Security Hub não é compatível com endpoints da VPC na região Asia Pacific (Osaka).

Criação de um endpoint da VPC de interface para o Security Hub

É possível criar um endpoint da VPC para o serviço Security Hub usando o console do Amazon VPC ou o AWS Command Line Interface (AWS CLI). Para mais informações, consulte Criar um endpoint de interface no Guia do usuário do AWS PrivateLink.

Crie um endpoint da VPC para o Security Hub usando o seguinte nome de serviço:

- com.amazonaws.*region*.securityhub

Se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API para o Security Hub usando seu nome DNS padrão para a região, por exemplo, `securityhub.us-east-1.amazonaws.com`.

Para mais informações, consulte Acessar um serviço por meio de um endpoint de interface no Guia do AWS PrivateLink.

Criar uma política de endpoint da VPC no Security Hub

É possível anexar uma política de endpoint do endpoint da VPC que controla o acesso ao Security Hub. Essa política especifica as seguintes informações:

- A entidade principal que pode executar ações.
- As ações que podem ser executadas.
- Os recursos sobre os quais as ações podem ser realizadas.

Para mais informações, consulte Controlar o acesso a serviços com endpoints da VPC no Guia AWS PrivateLink.

Exemplo: política de endpoint da VPC para ações do Security Hub

Veja a seguir um exemplo de uma política de endpoint para o Security Hub. Quando anexada a um endpoint, essa política concede acesso às ações indicadas do Security Hub para todos as entidades principais em todos os recursos.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

Sub-redes compartilhadas

Você não pode criar, descrever, modificar ou excluir endpoints da VPC em sub-redes que são compartilhadas com você. No entanto, você pode usar os endpoints da VPC em sub-redes que são compartilhadas com você. Para obter informações sobre o compartilhamento da VPC, consulte Compartilhar sua VPC com outras contas no Guia do usuário da Amazon VPC.

Registro de chamadas API do AWS Security Hub com o AWS CloudTrail

O AWS Security Hub é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um serviço da AWS no Security Hub. O CloudTrail captura as chamadas de API para o Security Hub como eventos. As chamadas capturadas incluem as do console do Security Hub e as de código para as operações de API do Security Hub. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o Security Hub. 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 para o Security Hub, o endereço IP no qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, além de detalhes adicionais.

Para saber mais sobre o CloudTrail, incluindo como configurá-lo e ativá-lo, consulte o AWS CloudTrail Guia do usuário do.

Informações do Security Hub no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando a atividade do evento compatível ocorre no Security Hub, ela é registrada em um evento do CloudTrail juntamente com outros eventos de serviços da AWS no Histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua conta . Para obter mais informações, consulte Viewing events with CloudTrail event history.

Para obter um registro contínuo de eventos em sua conta, incluindo eventos para o Security Hub, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões do AWS. A trilha registra eventos de todas as regiões na partição da AWS e entrega os arquivos de log no bucket do Amazon S3 que você especificou Além disso, é possível configurar outros serviços da AWS para analisar mais ainda e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para mais informações, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configuração notificações do Amazon SNS para o CloudTrail

- Como receber arquivos de log do CloudTrail de várias regiões e Como receber arquivos de log do CloudTrail de várias contas

O Security Hub é compatível com o log de todas as ações de API do Security Hub como eventos em logs do CloudTrail. Para visualizar uma lista de operações do Security Hub, consulte a Referência de API do Security Hub.

Quando uma atividade para as ações a seguir é registrada no CloudTrail, o valor de `responseElements` é definido como `null`. Isso garante que as informações confidenciais não sejam incluídas nos logs do CloudTrail.

- `BatchImportFindings`
- `GetFindings`
- `GetInsights`
- `GetMembers`
- `UpdateFindings`

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 um perfil ou de um usuário federado
- Se a solicitação foi feita por outro serviço da AWS

Para obter mais informações, consulte Elemento de identidade do usuário do CloudTrail.

Exemplo: entradas de arquivo de log do Security Hub

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 CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte, e inclui informações sobre a ação solicitada, data e hora da ação, parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública, portanto não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log CloudTrail que demonstra a `CreateInsight` ação. Neste exemplo, um insight chamado `Test Insight` será criado. O atributo `ResourceId` é especificado como o agregador Group by (Agrupar por) e nenhum filtro opcional para esse insight é especificado. Para obter mais informações sobre insights, consulte Insights no AWS Security Hub.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJK6U5DS22IAVUI7BW",
        "arn": "arn:aws:iam::012345678901:user/TestUser",
        "accountId": "012345678901",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "TestUser"
    },
    "eventTime": "2018-11-25T01:02:18Z",
    "eventSource": "securityhub.amazonaws.com",
    "eventName": "CreateInsight",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
    "requestParameters": {
        "Filters": {},
        "ResultField": "ResourceId",
        "Name": "Test Insight"
    },
    "responseElements": {
        "InsightArn": "arn:aws:securityhub:us-west-2:0123456789010:insight/custom/
f4c4890b-ac6b-4c26-95f9-e62cc46f3055"
    },
    "requestID": "c0fffccd-f04d-11e8-93fc-ddcd14710066",
    "eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "012345678901"
}
```

Marcar recursos do AWS Security Hub

Uma tag é uma etiqueta opcional que você define e atribui a recursos da AWS, incluindo certos tipos de recurso do AWS Security Hub. As tags podem ajudar a identificar, categorizar e gerenciar recursos de diferentes maneiras, como por finalidade, proprietário, ambiente ou outros critérios. Por exemplo, é possível usar tags para distinguir entre recursos, identificar recursos que aceitam determinados requisitos de conformidade ou fluxos de trabalho ou alocar custos.

É possível atribuir tags aos tipos de recursos do Security Hub a seguir: regras de automação, políticas de configuração e o recurso `Hub`.

Tópicos

Fundamentos das tags

Um recurso pode ter até 50 tags. Cada tag consiste em uma chave de tag obrigatória e um valor de tag opcional, ambos definidos por você. Uma chave de tag é um rótulo geral que atua como uma categoria para valores de tags mais específicos. Um valor de tag atua como um descritor de uma chave de tag.

Por exemplo, se você criar regras de automação diferentes para ambientes diferentes (um conjunto de regras de automação para contas de teste e outro para contas de produção), poderá atribuir uma chave de tag `Environment` a essas regras. O valor da tag associada pode ser `Test` para as regras associadas às contas de teste e `Prod` para as regras associadas às contas de produção e UOs.

Ao definir e atribuir tags aos recursos do AWS Security Hub, lembre-se do seguinte:

- Cada recurso pode ter um máximo de 50 tags.
- Em todos os recurso, cada chave de tag precisa ser exclusiva e ter apenas um valor de tag.

- As chaves e valores das tags diferenciam maiúsculas de minúsculas. Recomendamos definir uma estratégia para letras maiúsculas em tags e implementá-la de forma consistente em todos os recursos.
- Uma chave de tag pode ter no máximo 128 caracteres UTF-8. Um valor de tag pode ter no máximo 256 caracteres UTF-8. Os caracteres podem ser letras, números, espaços ou os seguintes símbolos: _ . : / = + - @
- O prefixo `aws:` é reservado para uso da AWS. Não é possível usá-lo em nenhuma chave ou valor de tag definido por você. Você também não pode editar ou remover chaves ou valores de tag que usam esse prefixo. As tags que usam esse prefixo não adicionam à cota de 50 tags por recurso.
- Todas as tags que você atribuir estão disponíveis somente para sua Conta da AWS e somente no(a) Região da AWS em que você as atribui.
- Se você atribuir tags a um recurso usando o Security Hub, as tags serão aplicadas somente ao recurso que está armazenado diretamente no Security Hub no(a) Região da AWS aplicável. Eles não são aplicados a nenhum recurso de suporte associado que o Security Hub cria, usa ou mantém para você em outros Serviços da AWS. Por exemplo, se você atribuir tags a uma regra de automação que atualiza descobertas relacionadas ao Amazon Simple Storage Service (Amazon S3), as tags são aplicadas somente à sua regra de automação no Security Hub para a região especificada. Elas não são aplicadas aos seus buckets do S3. Para também atribuir tags a um recurso associado, é possível usar AWS Resource Groups ou AWS service (Serviço da AWS) que armazena o recurso, por exemplo, Amazon S3 para um bucket do S3. A atribuição de tags aos recursos associados pode ajudar você a identificar recursos de suporte para seus recursos do Security Hub.
- Se você excluir um recurso, quaisquer tags atribuídas ao recurso também serão excluídas.

> **Important**
>
> Não armazene dados confidenciais ou outros tipos de dados sigilosos em tags. Muitos Serviços da AWS conseguem acessar as tags, incluindo AWS Billing and Cost Management. As tags não devem ser usadas para dados confidenciais.

Para adicionar e gerenciar tags para recursos do Security Hub, é possível usar o console do Security Hub, a API do Security Hub ou a API de aplicação de tags do AWS Resource Groups. Com o Security Hub é possível adicionar tags aos recursos ao criá-los. Você também pode adicionar e gerenciar tags para recursos individuais existentes. Com o Resource Groups é possível adicionar

e gerenciar tags em lote para vários recursos existentes, abrangendo vários Serviços da AWS, incluindo o Security Hub.

Para obter dicas sobre a aplicação de tags e práticas recomendadas, consulte Aplicação de tags nos seus recursos da AWS no Guia do usuário da aplicação de tags a recursos da AWS.

Como usar tags nas políticas do IAM

Depois de começar a colocar tags em recursos, defina permissões baseadas em tags a nível de recurso nas políticas AWS Identity and Access Management (IAM). Usando os tags dessa forma, é possível implementar um controle granular de quais usuários e funções em sua conta da Conta da AWS têm permissão para criar e marcar recursos, e quais usuários e funções têm permissão para criar, editar e remover tags de maneira mais geral. Para controlar o acesso com base em tags, é possível usar chaves de condição relacionadas à tag no elemento Condição das políticas do IAM.

Por exemplo, é possível criar uma política do IAM que permita que um usuário tenha acesso completo a todos os recursos do AWS Security Hub, se a tag `Owner` para o recurso especificar seu nome de usuário:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

Se você definir permissões em nível de recurso e baseadas em tag, elas entrarão em vigor imediatamente. Isso significa que seus recursos ficam mais seguros assim que são criados, e que é possível começar a aplicar rapidamente o uso de tags em novos recursos. Também é possível usar permissões em nível de recurso para controlar quais valores e chaves de tag podem ser associados a recursos novos e existentes. Para obter mais informações, consulte Controlar o acesso aos recursos da AWS usando tags no Guia do usuário do IAM.

Adicionar tags aos recursos do AWS Security Hub

Para adicionar tags a um recurso individual do AWS Security Hub, é possível usar o console ou a API do Security Hub. O console não aceita a adição de tags ao recurso Hub.

Para adicionar tags a vários recursos do Security Hub ao mesmo tempo, use as operações de tag da API de aplicação de tags do AWS Resource Groups.

> **Important**
>
> Adicionar tags a um recurso pode afetar o acesso a ele. Antes de adicionar uma tag a um recurso, revise todas as políticas do AWS Identity and Access Management (IAM) que possam usar tags para controlar o acesso aos recursos.

Console

Para adicionar uma tag a um recurso

Quando você cria uma regra de automação ou uma política de configuração, o console do Security Hub fornece opções para adicionar tags a ela. É possível fornecer a chave de tag e o valor da tag na seção Tags.

Security Hub API & AWS CLI

Para adicionar uma tag a um recurso

Para criar um recurso e adicionar uma ou mais tags a ele programaticamente, use a operação apropriada para o tipo de recurso que você deseja criar:

- Para criar uma política de configuração e adicionar uma ou mais tags a ela, invoque a API CreateConfigurationPolicy ou, se estiver usando a AWS CLI, execute o comando create-configuration-policy.
- Para criar uma regra de automação e adicionar uma ou mais tags a ela, invoque a API CreateAutomationRule ou, se estiver usando a AWS CLI, execute o comando create-automation-rule.
- Para habilitar o Security Hub e adicionar uma ou mais tags ao seu recurso Hub, invoque a API enableSecurityHub ou, se estiver usando a AWS Command Line Interface (AWS CLI), execute o comando enable-security-hub.

Em sua solicitação, use o parâmetro `tags` para especificar a chave da tag e o valor opcional da tag para cada tag a ser adicionada ao recurso. O parâmetro `tags` especifica uma matriz de objetos. Cada objeto especifica uma chave de tag e seu valor de tag associado.

Para adicionar uma ou mais tags a um recurso existente, use a operação TagResource da API do Security Hub ou, se estiver usando a AWS CLI, execute o comando tag-resource. Em sua solicitação, especifique o nome do recurso da Amazon (ARN) do recurso ao qual você deseja adicionar uma tag. Use o parâmetro `tags` para especificar a chave da tag (`key`) e o valor opcional da tag (`value`) para cada tag a ser adicionada. O parâmetro `tags` especifica uma matriz de objetos, um objeto para cada chave de tag e seu valor de tag associado.

Por exemplo, o comando AWS CLI a seguir adiciona uma chave de tag `Environment` com um valor de tag `Prod` à política de configuração especificada. Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha "barra invertida (\)" para melhorar a legibilidade.

Exemplo de comando da CLI:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Prod
```

Em que:

- `resource-arn` especifica o ARN da política de configuração à qual adicionar uma tag.
- *`Environment`* é a chave da tag a ser adicionada à regra.
- *`Prod`* é o valor da tag para a chave de tag especificada (*`Environment`*).

No exemplo a seguir, o comando adiciona várias tags à política de configuração.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Prod key=CostCenter,value=12345 key=Owner,value=jane-
doe
```

Para cada objeto em uma matriz `tags`, os argumentos `key` e `value` são obrigatórios. Entretanto, o valor do argumento `value` pode ser uma string vazia. Se você não quiser associar um valor a

uma chave, não especifique um valor para o argumento `value`. Por exemplo, o comando a seguir adiciona uma chave de tag `Owner` sem valor de tag associado:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Owner,value=
```

Se uma operação de atribuição de tag for bem-sucedida, o Security Hub dará uma resposta HTTP 200 vazia. Caso contrário, o Security Hub dará uma resposta HTTP 4 xx ou 500 que indica por que a operação falhou.

Revisão de tags para recursos do AWS Security Hub

É possível revisar as tags (tanto chaves de tag quanto valores de tag) de uma regra de automação ou política de configuração do Security Hub usando o console do Security Hub ou a API do Security Hub. O console não aceita a revisão de tags para o recurso `Hub`.

Para revisar tags de vários recursos do Security Hub ao mesmo tempo, use as operações de tag da API de aplicação de tags do AWS Resource Groups.

Console

Para revisar as tags de um recurso

1. Usando as credenciais do administrador do Security Hub, abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.
2. Realize uma das seguintes ações, dependendo do tipo de recurso que vai receber a tag:
   - Para revisar as tags de uma regra de automação, escolha Automações no painel de navegação. Em seguida, escolha uma regra de automação.
   - Para revisar as tags de uma política de configuração, escolha Configuração no painel de navegação. Em seguida, na guia Políticas, selecione a opção ao lado de uma política de configuração. Um painel lateral se abrirá, mostrando o número de tags atribuídas à política. É possível expandir o cabeçalho Tags para ver as chaves e os valores das tags.

A seção Tags lista todas as tags atribuídas ao recurso atualmente.

Security Hub API & AWS CLI

Para revisar as tags de um recurso

Para recuperar e revisar as tags de um recurso existente, invoque a API ListTagsForResource. Em sua solicitação, use o parâmetro `resourceArn` para especificar o nome do recurso da Amazon (ARN) do recurso.

Se você estiver usando a AWS CLI, execute o comando list-tags-for-resource e use o parâmetro `resource-arn` para especificar o ARN do recurso. Por exemplo:

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Se a operação ocorrer com êxito, o Security Hub dará uma matriz `tags`. Cada objeto na matriz especifica uma tag (tanto a chave de tag quanto o valor da tag) que está atualmente atribuída ao recurso. Por exemplo:

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Prod"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

Onde `Environment`, `CostCenter` e `Owner` são as chaves de tag atribuídas ao recurso. `Prod` é o valor da tag associado à chave da tag `Environment`. `12345` é o valor da tag associado à chave da tag `CostCenter`. A chave de tag `Owner` não tem nenhum valor associado.

Para exibir uma lista de todos os recursos do Security Hub que possuam tags, e todas as tags que estejam associadas a cada um desses recursos, use a operação GetResources

da API Tags do AWS Resource Groups. Na sua solicitação, defina o valor do parâmetro `ResourceTypeFilters` como `securityhub`. Para fazer isso usando o AWS CLI, execute o comando get-resources e defina o valor do parâmetro `resource-type-filters` como `securityhub`. Por exemplo:

```
$ aws resourcegroupstaggingapi get-resources -\-resource-type-filters "securityhub"
```

Se a operação obtiver êxito, o Resource Groups retornará uma matriz `ResourceTagMappingList`. A matriz contém um objeto para cada recurso do Security Hub que contenha tags. Cada objeto especifica o ARN de um recurso do Security Hub e as chaves e valores de tag atribuídos ao recurso.

Editar tags para recursos do AWS Security Hub

Para editar as tags (chaves de tag ou valores de tag) de um recurso do AWS Security Hub, é possível usar a API do Security Hub. Atualmente, o console do Security Hub não é compatível com a edição de tags.

Para editar tags de vários recursos do Security Hub ao mesmo tempo, use as operações de tag da API de aplicação de tags do AWS Resource Groups.

> **Important**
>
> Editar as tags de um recurso pode afetar o acesso a ele. Antes de editar a chave ou o valor de uma tag para um recurso, revise todas as políticas do AWS Identity and Access Management (IAM) que possam usar a tag para controlar o acesso aos recursos.

Security Hub API & AWS CLI

Para editar as tags de um recurso

Ao editar uma tag para um recurso programaticamente, você substitui a tag existente por novos valores. Portanto, a melhor maneira de editar uma tag depende se você deseja editar uma chave, um valor ou ambos. Para editar uma chave de tag, remova a tag atual e adicione uma nova tag.

Para editar ou remover somente o valor da tag associado a uma chave de tag, substitua o valor existente usando a operação TagResource da API do Security Hub. Se você estiver usando a

AWS CLI, execute o comando tag-resource. Em sua solicitação, especifique o nome do recurso da Amazon (ARN) do recurso cujo valor de tag deseja editar ou remover.

Para editar um valor de tag, use o parâmetro `tags` para especificar a chave de tag cujo valor de tag você deseja alterar. Você também deve especificar o novo valor da tag para a chave. Por exemplo, o comando da AWS CLI a seguir altera o valor da tag de `Prod` para `Test` da chave de tag `Environment` que é atribuída à regra de automação especificada: Este exemplo está formatado para Linux, macOS ou Unix e usa o caractere de continuação de linha de barra invertida (\) para melhorar a legibilidade.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Environment,value=Test
```

Em que:

- O `resource-arn` especifica o ARN da política de configuração.
- *`Environment`* é a chave de tag associada ao valor da tag a ser alterado.
- *`Test`* é o novo valor da chave especificada (*`Environment`*).

Para remover um valor de uma chave, não especifique um valor para o argumento `value` da chave no parâmetro `tags`. Por exemplo:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags key=Owner,value=
```

Se a operação for bem-sucedida, o Security Hub retornará uma resposta HTTP 200 vazia. Caso contrário, o Security Hub dará uma resposta HTTP 4 xx ou 500 que indica por que a operação falhou.

Remover tags dos recursos do AWS Security Hub

Para remover tags de um recurso do AWS Security Hub, é possível usar a API Security Hub. Atualmente, o console do Security Hub não é compatível com a remoção de tags.

Para remover tags de vários recursos do Security Hub ao mesmo tempo, use as operações de tag da API de aplicação de tags do AWS Resource Groups.

> **Important**
>
> Remover tags de um recurso pode afetar o acesso a ele. Antes de remover uma tag, revise todas as políticas do AWS Identity and Access Management (IAM) que possam usar a tag para controlar o acesso aos recursos.

Security Hub API & AWS CLI

Como remover as tags de um recurso

Para remover uma ou mais tags de um recurso de forma programática, use a operação UntagResource da API do Security Hub. Em sua solicitação, use o parâmetro `resourceArn` para especificar o nome do recurso da Amazon (ARN) do recurso para remover uma tag. Use o parâmetro `tagKeys` para especificar a chave da tag a ser removida. Para remover várias tags, anexe o parâmetro `tagKeys` e o argumento de cada tag a ser removida, separados por (&) — por exemplo, `tagKeys=key1&tagKeys=key2`. Para remover somente um valor de tag específico (não uma chave de tag) de um recurso, edite a tag em vez de removê-la.

Se você estiver usando a AWS CLI, execute o comando untag-resource para remover uma ou mais tags de um recurso. Para o parâmetro `resource-arn`, especifique o ARN do recurso do qual remover uma tag. Use o parâmetro `tag-keys` para especificar a chave da tag a ser removida. Por exemplo, o comando a seguir remove a tag `Environment` (tanto a chave quanto o valor da tag) da política de configuração especificada:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

Onde `resource-arn` especifica o ARN da política de configuração da qual remover uma tag e *`Environment`* é a chave da tag a ser removida.

Para remover várias tags de um recurso, acrescente cada chave adicional como argumento para o parâmetro `tag-keys`. Por exemplo:

```
$ aws securityhub untag-resource \
```

```
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment Owner
```

Se a operação for bem-sucedida, o Security Hub retornará uma resposta HTTP 200 vazia. Caso contrário, o Security Hub dará uma resposta HTTP 4 xx ou 500 que indica por que a operação falhou.

Cotas com o Security Hub

Sua Conta da AWS tem certas cotas padrão, anteriormente chamadas de limites, para cada AWS service (Serviço da AWS). Essas cotas são o número máximo de recursos de serviço ou operações da sua conta. Este tópico contém links para as cotas que se aplicam aos recursos e operações do Security Hub AWS para sua conta. A menos que especificado de outra forma, cada cota se aplica à sua conta em cada Região da AWS.

Algumas cotas podem ser aumentadas, enquanto outras não podem. Para solicitar um aumento a uma cota, use o console do Service Quotas. Para saber como solicitar um aumento, consulte Solicitar um aumento de cota no Guia do usuário do Service Quotas. Se uma cota não estiver disponível no console do Service Quotas, use o formulário de aumento do limite de serviço no AWS Support Center Console para solicitar um aumento na cota.

Cotas máximas

Para obter uma lista de cotas que se aplicam aos recursos do Security Hub, consulte endpoints e cotas do AWS Security Hub no Referência geral da AWS.

Cotas de tarifa

Para obter uma lista de cotas que se aplicam às operações da API do Security Hub, consulte a AWS Referência da API do Security Hub.

Se você configurou Agregação entre regiões, uma chamada para `BatchImportFindings` e `BatchUpdateFindings` afeta as regiões vinculadas e a região de agregação. A operação `GetFindings` recupera descobertas das regiões vinculadas e da região de agregação. No entanto, as operações `BatchEnableStandards` e `UpdateStandardsControl` são específicas da região.

Limites regionais do Security Hub

Alguns recursos do AWS Security Hub estão disponíveis apenas em alguns Regiões da AWS. As seções a seguir especificam esses limites regionais.

Para obter uma lista das regiões em que o Security Hub está disponível, consulte AWS Endpoints e cotas do Security Hub no Referência geral da AWS.

Restrições de agregação entre regiões

Em AWS GovCloud (US), a agregação entre regiões está disponível somente para descobertas, atualizações e insights AWS GovCloud (US) . Especificamente, você só pode agregar descobertas, atualizações e insights entre AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA).

Nas regiões da China, a agregação entre regiões está disponível somente para descobertas, atualizações de descobertas e insights das regiões da China. Especificamente, você só pode agregar descobertas, atualizações de descobertas e insights entre a China (Pequim) e a China (Ningxia).

Não é possível usar uma região desabilitada por padrão como sua região de agregação. Para obter uma lista de regiões desabilitadas por padrão, consulte Habilitar uma região no Referência geral da AWS.

Disponibilidade de integrações por região

Algumas integrações não estão disponíveis em todas as regiões Se uma integração não estiver disponível em uma região específica, ela não será listada na página Integrações do console do Security Hub quando você escolher essa região.

Integrações com suporte na China (Pequim) e na China (Ningxia)

As regiões China (Pequim) e China (Ningxia) oferecem suporte somente às seguintes integrações com serviços da AWS:

- AWS Firewall Manager
- Amazon GuardDuty
- AWS Identity and Access Management Access Analyzer

- Amazon Inspector
- AWS IoT Device Defender
- AWS Systems Manager Explorer
- AWS Systems Manager OpsCenter
- AWS Systems Manager Gerenciador de patches

As regiões China (Pequim) e China (Ningxia) são compatíveis somente com as seguintes integrações de terceiros:

- Cloud Custodian
- FireEye Helix
- Helecloud
- IBM QRadar
- PagerDuty
- Palo Alto Networks Cortex XSOAR
- Palo Alto Networks VM-Series
- Prowler
- RSA Archer
- Splunk Enterprise
- Splunk Phantom
- ThreatModeler

Integrações que são suportadas em AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA)

As regiões AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA) oferecem suporte somente às seguintes integrações com serviços: AWS

- AWS Config
- Amazon Detective
- AWS Firewall Manager
- Amazon GuardDuty

- AWS Health
- IAM Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender

As regiões AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA) oferecem suporte somente às seguintes integrações de terceiros:

- Atlassian Jira Service Management
- Atlassian Jira Service Management Cloud
- Atlassian OpsGenie
- Caveonix Cloud
- Cloud Custodian
- Cloud Storage Security Antivirus for Amazon S3
- CrowdStrike Falcon
- FireEye Helix
- Forcepoint CASB
- Forcepoint DLP
- Forcepoint NGFW
- Fugue
- Kion
- MicroFocus ArcSight
- NETSCOUT Cyber Investigator
- PagerDuty
- Palo Alto Networks – Prisma Cloud Compute
- Palo Alto Networks – Prisma Cloud Enterprise
- Palo Alto Networks – VM-Series(disponível somente em AWS GovCloud (Oeste dos EUA))
- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect
- RSA Archer

- SecureCloudDb
- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

Disponibilidade de padrões por região

Padrão gerenciado por serviços: AWS Control Tower está disponível somente em regiões que oferecem AWS Control Tower suporte, inclusive. AWS GovCloud (US) Para obter uma lista de regiões que AWS Control Tower oferecem suporte, consulte Como Regiões da AWS trabalhar com AWS Control Tower no Guia AWS Control Tower do usuário.

O Padrão AWS de Etiquetagem de Recursos não está disponível no Oeste do Canadá (Calgary), China e. AWS GovCloud (US)

Outros padrões de segurança estão disponíveis em todas as regiões nas quais o Security Hub está disponível.

Disponibilidade de controles por região

Os controles do Security Hub podem não estar disponíveis em todas as regiões. Para ver uma lista de controles indisponíveis em cada região, consulte Limites regionais de controles. Um controle não aparece na lista de controles no console do Security Hub se não estiver disponível na região em que você está conectado. A exceção é se você estiver conectado a uma região de agregação. Nesse caso, é possível ver os controles que estão disponíveis na região de agregação ou em uma ou mais regiões vinculadas.

Limites regionais de controles

AWS Os controles do Security Hub podem não estar disponíveis em todos Regiões da AWS. Esta página mostra quais controles não estão disponíveis em regiões específicas. Um controle não aparece na lista de controles no console do Security Hub se não estiver disponível na região em que você está conectado. A exceção é se você estiver conectado a uma região de agregação. Nesse caso, é possível ver os controles que estão disponíveis na região de agregação ou em uma ou mais regiões vinculadas.

Sumário

- América do Sul (São Paulo)
- AWS GovCloud (Leste dos EUA)
- AWS GovCloud (Oeste dos EUA)

Leste dos EUA (Norte da Virgínia)

Os controles a seguir não são compatíveis no Leste dos EUA (N. da Virgínia).

- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [ElastiCache.4] ElastiCache para Redis, os grupos de replicação devem ser criptografados em repouso
- [ElastiCache.5] ElastiCache para Redis, os grupos de replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache para grupos de replicação do Redis antes da versão 6.0 deve usar o Redis AUTH
- [ElastiCache.7] os ElastiCache clusters não devem usar o grupo de sub-rede padrão
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas

- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints

Leste dos EUA (Ohio)

Os controles a seguir não são compatíveis no Leste dos EUA (Ohio).

- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados

- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

Oeste dos EUA (N. da Califórnia)

Os controles a seguir não são compatíveis no Oeste dos EUA (N. da Califórnia).

- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado

- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos
- [DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch
- Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- Os endpoints do cluster EKS não devem ser acessíveis ao público
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes

- [FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

Oeste dos EUA (Oregon)

Os controles a seguir não são compatíveis no Oeste dos EUA (Oregon).

- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado

- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas

- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

África (Cidade do Cabo)

Os controles a seguir não são compatíveis na África (Cidade do Cabo).

- Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- [ApiGateway.1] O REST do API Gateway WebSocket e o registro de execução da API devem estar habilitados
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado
- [AppSync.5] As APIs AWS AppSync do GraphQL não devem ser autenticadas com chaves de API
- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas

- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais
- [CodeBuild.2] as variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- As instâncias de replicação do PCI.DMS.1 Database Migration Service não devem ser públicas
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos
- [DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch
- Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- [EC2.3] Os volumes anexados do Amazon EBS devem ser criptografados em repouso.
- As instâncias EC2 interrompidas devem ser removidas após um período de tempo especificado
- As instâncias do EC2 devem usar o Instance Metadata Service Version 2 (IMDSv2)
- [PCI.EC2.4] Os EIPs do EC2 não utilizados devem ser removidos
- [EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22
- [EC2.14] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 3389
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados

- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.1] O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS
- [EFS.2] Os volumes do Amazon EFS devem estar em planos de backup
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- Os endpoints do cluster EKS não devem ser acessíveis ao público
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [ELBv2.1] O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS
- [ELB.2] Os balanceadores de carga clássicos com ouvintes SSL/HTTPS devem usar um certificado fornecido pelo AWS Certificate Manager
- O Application Load Balancer deve ser configurado para eliminar cabeçalhos http
- [ELB.8] Os balanceadores de carga clássicos com ouvintes SSL devem usar uma política de segurança predefinida que tenha uma duração forte AWS Config
- [ELB.16] Os balanceadores de carga de aplicativos devem ser associados a uma ACL da web AWS WAF
- [EMR.1] Os nós primários do cluster do Amazon EMR não devem ter endereços IP públicos
- Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [GuardDuty.1] GuardDuty deve ser ativado
- [IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos
- [IAM.18] Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [IoT.1] perfis de AWS IoT Core segurança devem ser marcados
- [IoT.2] as ações de AWS IoT Core mitigação devem ser marcadas
- [IoT.3] as AWS IoT Core dimensões devem ser marcadas

- [IoT.4] os AWS IoT Core autorizadores devem ser marcados
- [IoT.5] aliases de AWS IoT Core função devem ser marcados
- As AWS IoT Core políticas [IoT.6] devem ser marcadas
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada
- Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público
- Os OpenSearch domínios [Opensearch.3] devem criptografar os dados enviados entre os nós
- O registro de erros de OpenSearch domínio [Opensearch.4] nos CloudWatch registros deve estar ativado
- Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado
- Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados
- Os OpenSearch domínios [Opensearch.7] devem ter um controle de acesso refinado ativado
- [Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [RDS.1] Os instantâneos do RDS devem ser privados
- [RDS.9] As instâncias de banco de dados do RDS devem publicar registros no Logs CloudWatch
- A autenticação do IAM deve ser configurada para instâncias do RDS
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1

- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [PCI.SSM.1] As instâncias do Amazon EC2 gerenciadas pelo devem ter um status de conformidade de patch de COMPLIANT (Em conformidade) após a instalação do patch
- PCI.SSM.2 As instâncias de Amazon EC2 gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras
- [WAF.11] O registro de ACL AWS WAF da web deve estar ativado

Ásia-Pacífico (Hong Kong)

Os controles a seguir não são compatíveis na Ásia-Pacífico (Hong Kong).

- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem

- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos
- [DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch
- Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- A autenticação do IAM deve ser configurada para instâncias do RDS
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado

- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [SES.1] As listas de contatos do SES devem ser marcadas
- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

Ásia-Pacífico (Hyderabad)

Os controles a seguir não são compatíveis na Ásia-Pacífico (Hyderabad).

- Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- [A conta.2] Contas da AWS deve fazer parte de uma organização AWS Organizations
- [ApiGateway.1] O REST do API Gateway WebSocket e o registro de execução da API devem estar habilitados
- Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end
- Os estágios da API REST de Gateway devem ter o rastreamento AWS X-Ray habilitado.

- O API Gateway deve ser associado a uma WAF Web ACL
- As rotas do API de Gateway devem especificar um tipo de autorização
- O registro de acesso deve ser configurado para os estágios V2 do API de Gateway
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado
- [AppSync.5] As APIs AWS AppSync do GraphQL não devem ser autenticadas com chaves de API
- [Athena.2] Os catálogos de dados do Athena devem ser marcados
- [Athena.3] Os grupos de trabalho do Athena devem ser marcados
- [AutoScaling.1] Grupos de Auto Scaling associados a um balanceador de carga devem usar verificações de integridade do ELB
- As instâncias do Amazon EC2 lançadas usando as configurações de execução em grupo do Auto Scaling não devem ter endereços IP públicos
- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.2] os pontos de AWS Backup recuperação devem ser marcados
- [Backup.3] os AWS Backup cofres devem ser marcados
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [Backup.5] os planos de AWS Backup backup devem ser marcados
- [CloudFormation.2] as CloudFormation pilhas devem ser marcadas
- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas

- [CloudTrail.6] Certifique-se de que o bucket do S3 usado para armazenar CloudTrail registros não esteja acessível ao público
- [CloudTrail.7] Certifique-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrail S3
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais
- [CodeBuild.2] as variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado
- [CodeBuild.3] Os registros do CodeBuild S3 devem ser criptografados
- [CodeBuild.4] ambientes de CodeBuild projeto devem ter uma duração de registro AWS Config
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [Detetive.1] Os gráficos do comportamento do detetive devem ser marcados
- As instâncias de replicação do PCI.DMS.1 Database Migration Service não devem ser públicas
- [DMS.2] Os certificados DMS devem ser marcados
- [DMS.3] As assinaturas de eventos do DMS devem ser marcadas
- [DMS.4] As instâncias de replicação do DMS devem ser marcadas
- [DMS.5] Os grupos de sub-redes de replicação do DMS devem ser marcados
- As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- Os endpoints do DMS devem usar SSL
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos

- [DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch
- Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- As tabelas do DynamoDB devem estar presentes em um plano de backup
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- [EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22
- [EC2.14] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 3389
- Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas
- [PCI.EC2.3] Os grupos de segurança do Amazon EC2 devem ser removidos
- Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- Os modelos de lançamento do Amazon EC2 não devem atribuir IPs públicos às interfaces de rede
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.34] As tabelas de rotas do gateway de trânsito EC2 devem ser marcadas
- [EC2.40] Os gateways NAT EC2 devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.51] Os endpoints da Client VPN do EC2 devem ter o registro em log de conexão do cliente habilitado
- Os repositórios privados do ECR devem ter a digitalização de imagens configurada
- [ECR.2] Os repositórios privados do ECR devem ter a imutabilidade da tag configurada
- Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário.
- As definições de tarefas do ECS devem ter uma configuração de registro em log
- [EFS.1] O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS
- [EFS.2] Os volumes do Amazon EFS devem estar em planos de backup
- Os pontos de acesso do EFS devem impor um diretório raiz
- Os pontos de acesso do EFS devem impor uma identidade de usuário

- [EFS.5] Os pontos de acesso do EFS devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- Os endpoints do cluster EKS não devem ser acessíveis ao público
- Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- O registro em log do Classic Load Balancer e Application Load Balancer deve estar ativado
- Balanceadores de carga de aplicações, redes e gateways não abrangem várias zonas de disponibilidade
- O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ElastiCache.1] Os clusters ElastiCache Redis devem ter o backup automático ativado
- [ElastiCache.6] ElastiCache para grupos de replicação do Redis antes da versão 6.0 deve usar o Redis AUTH
- [ElastiCache.7] os ElastiCache clusters não devem usar o grupo de sub-rede padrão
- [ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de integridade aprimorados habilitados
- [ElasticBeanstalk.2] As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas
- [ElasticBeanstalk.3] O Elastic Beanstalk deve transmitir registros para CloudWatch
- [EMR.1] Os nós primários do cluster do Amazon EMR não devem ter endereços IP públicos
- [ES.1] Os domínios do devem ter a criptografia em repouso habilitada.
- [ES.2] Os domínios do Elasticsearch não devem ser publicamente acessíveis
- Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós
- [ES.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado
- [EventBridge.2] ônibus de EventBridge eventos devem ser etiquetados
- [EventBridge.3] os ônibus de eventos EventBridge personalizados devem ter uma política baseada em recursos anexada
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups

- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- Os AWS Glue trabalhos [Glue.1] devem ser marcados
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] Os GuardDuty IPsets devem ser marcados
- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [IAM.1] As políticas do não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do não devem ter políticas do IAM anexadas
- [IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos
- [IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console
- As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.18] Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support
- [PCI.IAM.6] A MFA deve estar habilitada para todos os usuários do
- As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.24] As funções do IAM devem ser marcadas
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloudShellFullAccess
- [IoT.1] perfis de AWS IoT Core segurança devem ser marcados
- [IoT.2] as ações de AWS IoT Core mitigação devem ser marcadas
- [IoT.3] as AWS IoT Core dimensões devem ser marcadas
- [IoT.4] os AWS IoT Core autorizadores devem ser marcados
- [IoT.5] aliases de AWS IoT Core função devem ser marcados
- As AWS IoT Core políticas [IoT.6] devem ser marcadas
- Os fluxos do Kinesis devem ser criptografados em repouso
- As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS

- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- [Macie.1] O Amazon Macie deve estar ativado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve ser ativada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- [MQ.4] Os corretores do Amazon MQ devem ser marcados
- Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- [MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch
- Os instantâneos do cluster de banco de dados Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- Os clusters de banco de dados Neptune devem ter backups automatizados habilitados
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.7] Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- [Neptune.9] Os clusters de banco de dados do Neptune devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.1] Os firewalls do Network Firewall devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.2] O registro do Firewall de Rede deve estar ativado
- [NetworkFirewall.3] As políticas de Firewall de Rede devem ter pelo menos um grupo de regras associado
- [NetworkFirewall.4] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar pacotes completos

- [NetworkFirewall.5] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar para pacotes fragmentados
- [NetworkFirewall.6] O grupo de regras do Stateless Network Firewall não deve estar vazio
- [NetworkFirewall.9] Os firewalls do Firewall de Rede devem ter a proteção contra exclusão ativada
- Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada
- Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público
- Os OpenSearch domínios [Opensearch.3] devem criptografar os dados enviados entre os nós
- O registro de erros de OpenSearch domínio [Opensearch.4] nos CloudWatch registros deve estar ativado
- Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado
- Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados
- Os OpenSearch domínios [Opensearch.7] devem ter um controle de acesso refinado ativado
- [Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente
- Os OpenSearch domínios [Opensearch.9] devem ser marcados
- Os OpenSearch domínios [Opensearch.10] devem ter a atualização de software mais recente instalada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [RDS.2] As instâncias de banco de dados do RDS devem proibir o acesso público, conforme determinado pela duração PubliclyAccessible AWS Config
- [RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada
- [RDS.9] As instâncias de banco de dados do RDS devem publicar registros no Logs CloudWatch
- A autenticação do IAM deve ser configurada para instâncias do RDS
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.15] Os clusters de banco de dados do RDS devem ser configurados para várias zonas de disponibilidade
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup

- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [RDS.28] Os clusters de banco de dados do RDS devem ser marcados
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [RDS.34] Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch
- Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [PCI.Redshift.1] Os clusters do devem proibir o acesso público
- As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito
- Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados
- O Amazon Redshift deve ter as atualizações automáticas para as versões principais habilitadas
- Os clusters do Redshift devem usar roteamento de VPC aprimorado
- [Redshift.10] Os clusters do Redshift devem ser criptografados em repouso
- [Redshift.12] As assinaturas de notificação de eventos do Redshift devem ser marcadas
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.6] As políticas de bucket de uso geral do S3 devem restringir o acesso a outros Contas da AWS
- [S3.17] Os buckets de uso geral do S3 devem ser criptografados em repouso com AWS KMS keys
- [SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet
- [SageMaker.2] as instâncias do SageMaker notebook devem ser iniciadas em uma VPC personalizada
- [SageMaker.3] Os usuários não devem ter acesso root às instâncias do SageMaker notebook
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [SES.1] As listas de contatos do SES devem ser marcadas
- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS

- [SNS.3] Os tópicos do SNS devem ser marcados
- As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas SQS devem ser marcadas
- [SSM.1] As instâncias do Amazon EC2 devem ser gerenciadas por AWS Systems Manager
- [PCI.SSM.1] As instâncias do Amazon EC2 gerenciadas pelo devem ter um status de conformidade de patch de COMPLIANT (Em conformidade) após a instalação do patch
- PCI.SSM.2 As instâncias de Amazon EC2 gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [StepFunctions.1] As máquinas de estado do Step Functions devem ter o registro ativado
- Os AWS Transfer Family fluxos de trabalho [Transfer.1] devem ser marcados
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.2] As regras regionais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.3] Os grupos de regras regionais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.4] As ACLs regionais AWS WAF clássicas da web devem ter pelo menos uma regra ou grupo de regras
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras
- [WAF.10] as ACLs AWS WAF da web devem ter pelo menos uma regra ou grupo de regras
- [WAF.11] O registro de ACL AWS WAF da web deve estar ativado

Ásia-Pacífico (Jacarta)

Os controles a seguir não são compatíveis na Ásia-Pacífico (Jacarta).

- [A conta.2] Contas da AWS deve fazer parte de uma organização AWS Organizations
- [ApiGateway.1] O REST do API Gateway WebSocket e o registro de execução da API devem estar habilitados
- Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end

- Os estágios da API REST de Gateway devem ter o rastreamento AWS X-Ray habilitado.
- O API Gateway deve ser associado a uma WAF Web ACL
- As rotas do API de Gateway devem especificar um tipo de autorização
- O registro de acesso deve ser configurado para os estágios V2 do API de Gateway
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado
- [AppSync.5] As APIs AWS AppSync do GraphQL não devem ser autenticadas com chaves de API
- [AutoScaling.3] As configurações de lançamento de grupos do Auto Scaling devem configurar as instâncias do EC2 para exigir o Instance Metadata Service Version 2 (IMDSv2)
- [AutoScaling.6] Os grupos de Auto Scaling devem usar vários tipos de instância em várias zonas de disponibilidade
- [AutoScaling.9] Os grupos do Amazon EC2 Auto Scaling devem usar os modelos de lançamento do Amazon EC2
- As instâncias do Amazon EC2 lançadas usando as configurações de execução em grupo do Auto Scaling não devem ter endereços IP públicos
- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.2] os pontos de AWS Backup recuperação devem ser marcados
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [Backup.5] os planos de AWS Backup backup devem ser marcados
- [CloudFormation.2] as CloudFormation pilhas devem ser marcadas
- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3

- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CloudWatch.17] ações de CloudWatch alarme devem ser ativadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais
- [CodeBuild.2] as variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado
- [CodeBuild.3] Os registros do CodeBuild S3 devem ser criptografados
- [CodeBuild.4] ambientes de CodeBuild projeto devem ter uma duração de registro AWS Config
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [Detetive.1] Os gráficos do comportamento do detetive devem ser marcados
- As instâncias de replicação do PCI.DMS.1 Database Migration Service não devem ser públicas
- [DMS.2] Os certificados DMS devem ser marcados
- [DMS.3] As assinaturas de eventos do DMS devem ser marcadas
- [DMS.4] As instâncias de replicação do DMS devem ser marcadas
- [DMS.5] Os grupos de sub-redes de replicação do DMS devem ser marcados
- As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- Os endpoints do DMS devem usar SSL
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos

- [DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch
- Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- As tabelas do DynamoDB devem estar presentes em um plano de backup
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- [EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22
- [EC2.14] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 3389
- Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas
- [PCI.EC2.3] Os grupos de segurança do Amazon EC2 devem ser removidos
- Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.51] Os endpoints da Client VPN do EC2 devem ter o registro em log de conexão do cliente habilitado
- Os repositórios privados do ECR devem ter a digitalização de imagens configurada
- [ECR.2] Os repositórios privados do ECR devem ter a imutabilidade da tag configurada
- Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- Os serviços do ECS não devem ter endereços IP públicos atribuídos a eles automaticamente
- As definições de tarefas do ECS não devem compartilhar o namespace do processo do host
- Os contêineres ECS devem ser executados sem privilégios
- Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz
- Os segredos não devem ser passados como variáveis de ambiente do contêiner
- As definições de tarefas do ECS devem ter uma configuração de registro em log
- Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate
- Os clusters do ECS devem usar Container Insights
- [EFS.1] O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS
- [EFS.2] Os volumes do Amazon EFS devem estar em planos de backup

- Os pontos de acesso do EFS devem impor um diretório raiz
- Os pontos de acesso do EFS devem impor uma identidade de usuário
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- Os endpoints do cluster EKS não devem ser acessíveis ao público
- Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- Balanceadores de carga de aplicações, redes e gateways não abrangem várias zonas de disponibilidade
- O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ElastiCache.1] Os clusters ElastiCache Redis devem ter o backup automático ativado
- [ElastiCache.6] ElastiCache para grupos de replicação do Redis antes da versão 6.0 deve usar o Redis AUTH
- [ElastiCache.7] os ElastiCache clusters não devem usar o grupo de sub-rede padrão
- [ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de integridade aprimorados habilitados
- [ElasticBeanstalk.2] As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas
- [EMR.1] Os nós primários do cluster do Amazon EMR não devem ter endereços IP públicos
- [ES.1] Os domínios do devem ter a criptografia em repouso habilitada.
- [ES.2] Os domínios do Elasticsearch não devem ser publicamente acessíveis
- Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- Os AWS Glue trabalhos [Glue.1] devem ser marcados
- [GuardDuty.2] GuardDuty os filtros devem ser marcados

- [GuardDuty.3] Os GuardDuty IPsets devem ser marcados
- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [IAM.18] Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [IoT.1] perfis de AWS IoT Core segurança devem ser marcados
- [IoT.2] as ações de AWS IoT Core mitigação devem ser marcadas
- [IoT.3] as AWS IoT Core dimensões devem ser marcadas
- [IoT.4] os AWS IoT Core autorizadores devem ser marcados
- [IoT.5] aliases de AWS IoT Core função devem ser marcados
- As AWS IoT Core políticas [IoT.6] devem ser marcadas
- Os fluxos do Kinesis devem ser criptografados em repouso
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- [Macie.1] O Amazon Macie deve estar ativado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve ser ativada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- [MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch
- Os instantâneos do cluster de banco de dados Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- Os clusters de banco de dados Neptune devem ter backups automatizados habilitados
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.7] Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos

- [Neptune.9] Os clusters de banco de dados do Neptune devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.1] Os firewalls do Network Firewall devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.3] As políticas de Firewall de Rede devem ter pelo menos um grupo de regras associado
- [NetworkFirewall.4] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar pacotes completos
- [NetworkFirewall.5] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar para pacotes fragmentados
- [NetworkFirewall.6] O grupo de regras do Stateless Network Firewall não deve estar vazio
- Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada
- Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público
- Os OpenSearch domínios [Opensearch.3] devem criptografar os dados enviados entre os nós
- O registro de erros de OpenSearch domínio [Opensearch.4] nos CloudWatch registros deve estar ativado
- Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado
- Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados
- Os OpenSearch domínios [Opensearch.7] devem ter um controle de acesso refinado ativado
- [Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [RDS.9] As instâncias de banco de dados do RDS devem publicar registros no Logs CloudWatch
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [PCI.Redshift.1] Os clusters do devem proibir o acesso público
- As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito

- Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados
- Os clusters do Redshift devem usar roteamento de VPC aprimorado
- [Redshift.9] Os clusters do Redshift não devem usar o nome do banco de dados padrão
- [Redshift.10] Os clusters do Redshift devem ser criptografados em repouso
- [Redshift.12] As assinaturas de notificação de eventos do Redshift devem ser marcadas
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.11] Os buckets de uso geral do S3 devem ter as notificações de eventos ativadas
- [S3.13] Os buckets de uso geral do S3 devem ter configurações de ciclo de vida
- [SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet
- [SageMaker.2] as instâncias do SageMaker notebook devem ser iniciadas em uma VPC personalizada
- [SageMaker.3] Os usuários não devem ter acesso root às instâncias do SageMaker notebook
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [SNS.3] Os tópicos do SNS devem ser marcados
- As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas SQS devem ser marcadas
- [SSM.1] As instâncias do Amazon EC2 devem ser gerenciadas por AWS Systems Manager
- [PCI.SSM.1] As instâncias do Amazon EC2 gerenciadas pelo devem ter um status de conformidade de patch de COMPLIANT (Em conformidade) após a instalação do patch
- PCI.SSM.2 As instâncias de Amazon EC2 gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.2] As regras regionais AWS WAF clássicas devem ter pelo menos uma condição

- [WAF.3] Os grupos de regras regionais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.4] As ACLs regionais AWS WAF clássicas da web devem ter pelo menos uma regra ou grupo de regras
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras
- [WAF.10] as ACLs AWS WAF da web devem ter pelo menos uma regra ou grupo de regras
- [WAF.11] O registro de ACL AWS WAF da web deve estar ativado

Ásia-Pacífico (Mumbai)

Os controles a seguir não são compatíveis na Ásia-Pacífico (Mumbai).

- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado

- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

Ásia-Pacífico (Melbourne)

Os controles a seguir não são compatíveis na Ásia-Pacífico (Melbourne).

- Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- O API Gateway deve ser associado a uma WAF Web ACL
- As rotas do API de Gateway devem especificar um tipo de autorização
- O registro de acesso deve ser configurado para os estágios V2 do API de Gateway
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado
- [AppSync.4] As APIs AWS AppSync do GraphQL devem ser marcadas
- [AppSync.5] As APIs AWS AppSync do GraphQL não devem ser autenticadas com chaves de API
- [Athena.2] Os catálogos de dados do Athena devem ser marcados
- [Athena.3] Os grupos de trabalho do Athena devem ser marcados
- [AutoScaling.1] Grupos de Auto Scaling associados a um balanceador de carga devem usar verificações de integridade do ELB
- As instâncias do Amazon EC2 lançadas usando as configurações de execução em grupo do Auto Scaling não devem ter endereços IP públicos
- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.2] os pontos de AWS Backup recuperação devem ser marcados
- [Backup.3] os AWS Backup cofres devem ser marcados
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [Backup.5] os planos de AWS Backup backup devem ser marcados
- [CloudFormation.2] as CloudFormation pilhas devem ser marcadas
- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados

- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais
- [CodeBuild.2] as variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado
- [CodeBuild.3] Os registros do CodeBuild S3 devem ser criptografados
- [CodeBuild.4] ambientes de CodeBuild projeto devem ter uma duração de registro AWS Config
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [Detetive.1] Os gráficos do comportamento do detetive devem ser marcados
- As instâncias de replicação do PCI.DMS.1 Database Migration Service não devem ser públicas
- [DMS.2] Os certificados DMS devem ser marcados
- [DMS.3] As assinaturas de eventos do DMS devem ser marcadas
- [DMS.4] As instâncias de replicação do DMS devem ser marcadas
- [DMS.5] Os grupos de sub-redes de replicação do DMS devem ser marcados
- As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- Os endpoints do DMS devem usar SSL
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado

- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos
- [DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch
- Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- As tabelas do DynamoDB devem estar presentes em um plano de backup
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- [PCI.EC2.1] Os instantâneos do Amazon EBS não devem ser restauráveis publicamente
- As instâncias EC2 interrompidas devem ser removidas após um período de tempo especificado
- As instâncias do EC2 devem usar o Instance Metadata Service Version 2 (IMDSv2)
- As instâncias do Amazon EC2 não devem ter um endereço IPv4 público
- [EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22
- [EC2.14] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 3389
- Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas
- [PCI.EC2.3] Os grupos de segurança do Amazon EC2 devem ser removidos
- Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- Os modelos de lançamento do Amazon EC2 não devem atribuir IPs públicos às interfaces de rede
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.33] Os anexos do gateway de trânsito EC2 devem ser marcados
- [EC2.34] As tabelas de rotas do gateway de trânsito EC2 devem ser marcadas
- [EC2.40] Os gateways NAT EC2 devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.51] Os endpoints da Client VPN do EC2 devem ter o registro em log de conexão do cliente habilitado
- [EC2.52] Os gateways de trânsito do EC2 devem ser marcados
- Os repositórios privados do ECR devem ter a digitalização de imagens configurada

- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário.
- As definições de tarefas do ECS devem ter uma configuração de registro em log
- [EFS.1] O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS
- [EFS.2] Os volumes do Amazon EFS devem estar em planos de backup
- Os pontos de acesso do EFS devem impor um diretório raiz
- Os pontos de acesso do EFS devem impor uma identidade de usuário
- [EFS.5] Os pontos de acesso do EFS devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- Os endpoints do cluster EKS não devem ser acessíveis ao público
- Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [EKS.6] Os clusters EKS devem ser marcados
- [EKS.7] As configurações do provedor de identidade EKS devem ser marcadas
- [EKS.8] Os clusters do EKS devem ter o registro em log de auditoria habilitado
- Balanceadores de carga de aplicações, redes e gateways não abrangem várias zonas de disponibilidade
- O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ElastiCache.1] Os clusters ElastiCache Redis devem ter o backup automático ativado
- [ElastiCache.2] ElastiCache para clusters de cache Redis deve ter a atualização automática de versão secundária habilitada
- [ElastiCache.3] ElastiCache para grupos de replicação do Redis, o failover automático deve estar ativado
- [ElastiCache.4] ElastiCache para Redis, os grupos de replicação devem ser criptografados em repouso
- [ElastiCache.5] ElastiCache para Redis, os grupos de replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache para grupos de replicação do Redis antes da versão 6.0 deve usar o Redis AUTH

- [ElastiCache.7] os ElastiCache clusters não devem usar o grupo de sub-rede padrão
- [ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de integridade aprimorados habilitados
- [ElasticBeanstalk.2] As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas
- [ElasticBeanstalk.3] O Elastic Beanstalk deve transmitir registros para CloudWatch
- [EMR.1] Os nós primários do cluster do Amazon EMR não devem ter endereços IP públicos
- [ES.1] Os domínios do devem ter a criptografia em repouso habilitada.
- [ES.2] Os domínios do Elasticsearch não devem ser publicamente acessíveis
- Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós
- [ES.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado
- [EventBridge.2] ônibus de EventBridge eventos devem ser etiquetados
- [EventBridge.3] os ônibus de eventos EventBridge personalizados devem ter uma política baseada em recursos anexada
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- Os AWS Glue trabalhos [Glue.1] devem ser marcados
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] Os GuardDuty IPsets devem ser marcados
- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [IAM.1] As políticas do não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do não devem ter políticas do IAM anexadas
- [IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos
- [IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- [IAM.7] As políticas de senha para usuários do IAM devem ter configurações fortes
- As credenciais de usuário do IAM não utilizadas devem ser removidas

- [IAM.10] As políticas de senha para usuários do IAM devem ter durações fortes AWS Config
- 1.5 Certifique-se de que política de senha do IAM exija pelo menos uma letra maiúscula
- 1.6 Certifique-se de que política de senha do IAM exija pelo menos uma letra minúscula
- 1.7 Certifique-se de que política de senha do IAM exija pelo menos um símbolo
- Certifique-se de que política de senha do IAM exija pelo menos um número
- 1.9 Certifique-se de que a política de senha do IAM exija um comprimento mínimo de 14 ou mais
- 1.10 Certifique-se de que a política de senha do IAM impeça a reutilização de senhas
- 1.11 Certifique-se de que a política de senha do IAM expire senhas em até 90 dias ou menos
- [IAM.18] Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support
- [PCI.IAM.6] A MFA deve estar habilitada para todos os usuários do
- As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.24] As funções do IAM devem ser marcadas
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloudShellFullAccess
- [IoT.1] perfis de AWS IoT Core segurança devem ser marcados
- [IoT.2] as ações de AWS IoT Core mitigação devem ser marcadas
- [IoT.3] as AWS IoT Core dimensões devem ser marcadas
- [IoT.4] os AWS IoT Core autorizadores devem ser marcados
- [IoT.5] aliases de AWS IoT Core função devem ser marcados
- As AWS IoT Core políticas [IoT.6] devem ser marcadas
- Os fluxos do Kinesis devem ser criptografados em repouso
- As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- [Macie.1] O Amazon Macie deve estar ativado

- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve ser ativada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- [MQ.4] Os corretores do Amazon MQ devem ser marcados
- Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- [MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch
- Os instantâneos do cluster de banco de dados Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- Os clusters de banco de dados Neptune devem ter backups automatizados habilitados
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.7] Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- [Neptune.9] Os clusters de banco de dados do Neptune devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.1] Os firewalls do Network Firewall devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.2] O registro do Firewall de Rede deve estar ativado
- [NetworkFirewall.3] As políticas de Firewall de Rede devem ter pelo menos um grupo de regras associado
- [NetworkFirewall.4] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar pacotes completos
- [NetworkFirewall.5] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar para pacotes fragmentados
- [NetworkFirewall.6] O grupo de regras do Stateless Network Firewall não deve estar vazio

- [NetworkFirewall.9] Os firewalls do Firewall de Rede devem ter a proteção contra exclusão ativada
- Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada
- Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público
- Os OpenSearch domínios [Opensearch.3] devem criptografar os dados enviados entre os nós
- O registro de erros de OpenSearch domínio [Opensearch.4] nos CloudWatch registros deve estar ativado
- Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado
- Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados
- Os OpenSearch domínios [Opensearch.7] devem ter um controle de acesso refinado ativado
- [Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente
- Os OpenSearch domínios [Opensearch.9] devem ser marcados
- Os OpenSearch domínios [Opensearch.10] devem ter a atualização de software mais recente instalada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [RDS.1] Os instantâneos do RDS devem ser privados
- [RDS.3] As instâncias de banco de dados do RDS devem ter a criptografia em repouso habilitada.
- [RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada
- A autenticação do IAM deve ser configurada para instâncias do RDS
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.15] Os clusters de banco de dados do RDS devem ser configurados para várias zonas de disponibilidade
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [RDS.28] Os clusters de banco de dados do RDS devem ser marcados
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [RDS.34] Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch

- Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [Redshift.12] As assinaturas de notificação de eventos do Redshift devem ser marcadas
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.14] Os buckets de uso geral do S3 devem ter o controle de versão ativado
- [S3.15] Os buckets de uso geral do S3 devem ter o Object Lock ativado
- [SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet
- [SageMaker.2] as instâncias do SageMaker notebook devem ser iniciadas em uma VPC personalizada
- [SageMaker.3] Os usuários não devem ter acesso root às instâncias do SageMaker notebook
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [SES.1] As listas de contatos do SES devem ser marcadas
- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [SNS.1] Os tópicos do SNS devem ser criptografados em repouso usando AWS KMS
- [SNS.3] Os tópicos do SNS devem ser marcados
- As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas SQS devem ser marcadas
- [PCI.SSM.1] As instâncias do Amazon EC2 gerenciadas pelo devem ter um status de conformidade de patch de COMPLIANT (Em conformidade) após a instalação do patch
- PCI.SSM.2 As instâncias de Amazon EC2 gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- Os documentos SSM não devem ser públicos
- [StepFunctions.1] As máquinas de estado do Step Functions devem ter o registro ativado
- [StepFunctions.2] As atividades do Step Functions devem ser marcadas
- Os AWS Transfer Family fluxos de trabalho [Transfer.1] devem ser marcados

- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras
- [WAF.11] O registro de ACL AWS WAF da web deve estar ativado

Asia Pacific (Osaka)

Os controles a seguir não são compatíveis na Ásia-Pacífico (Osaka).

- Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- [A conta.2] Contas da AWS deve fazer parte de uma organização AWS Organizations
- [ApiGateway.1] O REST do API Gateway WebSocket e o registro de execução da API devem estar habilitados
- Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end
- Os estágios da API REST de Gateway devem ter o rastreamento AWS X-Ray habilitado.
- O API Gateway deve ser associado a uma WAF Web ACL
- As instâncias do Amazon EC2 lançadas usando as configurações de execução em grupo do Auto Scaling não devem ter endereços IP públicos
- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [CloudFormation.2] as CloudFormation pilhas devem ser marcadas
- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados

- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CloudWatch.15] CloudWatch os alarmes devem ter ações especificadas configuradas
- [CloudWatch.16] os grupos de CloudWatch registros devem ser mantidos por um período de tempo especificado
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais
- [CodeBuild.2] as variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado
- [CodeBuild.3] Os registros do CodeBuild S3 devem ser criptografados
- [CodeBuild.4] ambientes de CodeBuild projeto devem ter uma duração de registro AWS Config
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [Detetive.1] Os gráficos do comportamento do detetive devem ser marcados
- As instâncias de replicação do PCI.DMS.1 Database Migration Service não devem ser públicas
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos

- [DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch
- Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- [DynamoDB.2] As tabelas do DynamoDB devem ter a recuperação ativada point-in-time
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- As tabelas do DynamoDB devem estar presentes em um plano de backup
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- [PCI.EC2.1] Os instantâneos do Amazon EBS não devem ser restauráveis publicamente
- [EC2.3] Os volumes anexados do Amazon EBS devem ser criptografados em repouso.
- As instâncias EC2 interrompidas devem ser removidas após um período de tempo especificado
- [EC2.7] A criptografia padrão do EBS deve estar ativada
- As instâncias do EC2 devem usar o Instance Metadata Service Version 2 (IMDSv2)
- As instâncias do Amazon EC2 não devem ter um endereço IPv4 público
- O Amazon EC2 deve ser configurado para usar endpoints da VPC criados para o serviço Amazon EC2
- [EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22
- [EC2.14] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 3389
- As sub-redes do Amazon EC2 não devem atribuir automaticamente endereços IP públicos
- As listas de controle de acesso à rede não utilizadas devem ser removidas
- As instâncias do Amazon EC2 não devem usar vários ENIs
- Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas
- [EC2.20] Ambos os túneis VPN para uma conexão VPN Site-to-Site devem estar ativos AWS
- [PCI.EC2.3] Os grupos de segurança do Amazon EC2 devem ser removidos
- Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.51] Os endpoints da Client VPN do EC2 devem ter o registro em log de conexão do cliente habilitado
- [EC2.52] Os gateways de trânsito do EC2 devem ser marcados
- Os repositórios privados do ECR devem ter a digitalização de imagens configurada
- [ECR.2] Os repositórios privados do ECR devem ter a imutabilidade da tag configurada

- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário.
- Os serviços do ECS não devem ter endereços IP públicos atribuídos a eles automaticamente
- As definições de tarefas do ECS não devem compartilhar o namespace do processo do host
- Os contêineres ECS devem ser executados sem privilégios
- Os segredos não devem ser passados como variáveis de ambiente do contêiner
- As definições de tarefas do ECS devem ter uma configuração de registro em log
- Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate
- Os clusters do ECS devem usar Container Insights
- [EFS.1] O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS
- [EFS.2] Os volumes do Amazon EFS devem estar em planos de backup
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- Os endpoints do cluster EKS não devem ser acessíveis ao público
- Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [ELBv2.1] O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS
- [ELB.2] Os balanceadores de carga clássicos com ouvintes SSL/HTTPS devem usar um certificado fornecido pelo AWS Certificate Manager
- Os receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS
- O Application Load Balancer deve ser configurado para eliminar cabeçalhos http
- [ELB.6] Os balanceadores de carga de aplicativos, gateways e redes devem ter a proteção contra exclusão ativada
- [ELB.8] Os balanceadores de carga clássicos com ouvintes SSL devem usar uma política de segurança predefinida que tenha uma duração forte AWS Config
- Os Classic Load Balancers devem ter o balanceador de carga entre zonas habilitado
- [ELB.16] Os balanceadores de carga de aplicativos devem ser associados a uma ACL da web AWS WAF
- [ElastiCache.1] Os clusters ElastiCache Redis devem ter o backup automático ativado
- [ElastiCache.7] os ElastiCache clusters não devem usar o grupo de sub-rede padrão

- [ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de integridade aprimorados habilitados
- [ElasticBeanstalk.2] As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas
- [ElasticBeanstalk.3] O Elastic Beanstalk deve transmitir registros para CloudWatch
- [EMR.1] Os nós primários do cluster do Amazon EMR não devem ter endereços IP públicos
- [ES.1] Os domínios do devem ter a criptografia em repouso habilitada.
- [ES.2] Os domínios do Elasticsearch não devem ser publicamente acessíveis
- Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós
- [FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [GuardDuty.1] GuardDuty deve ser ativado
- [IAM.4] A chave de acesso do usuário raiz do não deve existir
- [IAM.18] Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support
- As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [IoT.1] perfis de AWS IoT Core segurança devem ser marcados
- [IoT.2] as ações de AWS IoT Core mitigação devem ser marcadas
- [IoT.3] as AWS IoT Core dimensões devem ser marcadas
- [IoT.4] os AWS IoT Core autorizadores devem ser marcados
- [IoT.5] aliases de AWS IoT Core função devem ser marcados
- As AWS IoT Core políticas [IoT.6] devem ser marcadas
- Os fluxos do Kinesis devem ser criptografados em repouso
- As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS

- [KMS.3] não AWS KMS keys deve ser excluído acidentalmente
- [PCI.lambda.1] As funções do devem proibir o acesso público
- [Lambda.2] As funções do devem usar os tempos de execução mais recentes
- [PCI.Lambda.2] As funções do Lambda devem estar em uma VPC
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch
- Os instantâneos do cluster de banco de dados Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- Os clusters de banco de dados Neptune devem ter backups automatizados habilitados
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.7] Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- [Neptune.9] Os clusters de banco de dados do Neptune devem ser implantados em várias zonas de disponibilidade
- Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada
- Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público
- Os OpenSearch domínios [Opensearch.3] devem criptografar os dados enviados entre os nós
- O registro de erros de OpenSearch domínio [Opensearch.4] nos CloudWatch registros deve estar ativado
- Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado
- Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados
- Os OpenSearch domínios [Opensearch.7] devem ter um controle de acesso refinado ativado
- [Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados

- [RDS.1] Os instantâneos do RDS devem ser privados
- Os instantâneos do cluster do RDS e os instantâneos do banco de dados devem ser criptografados em repouso
- O monitoramento aprimorado deve ser configurado para instâncias de banco de dados do RDS
- [RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada
- [RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada
- [RDS.9] As instâncias de banco de dados do RDS devem publicar registros no Logs CloudWatch
- A autenticação do IAM deve ser configurada para instâncias do RDS
- A autenticação do IAM deve ser configurada para instâncias do RDS
- [RDS.13] As atualizações automáticas de versões secundárias do RDS devem ser ativadas
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.15] Os clusters de banco de dados do RDS devem ser configurados para várias zonas de disponibilidade
- As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [PCI.Redshift.1] Os clusters do devem proibir o acesso público
- As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito
- Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados
- Os clusters do Redshift devem usar roteamento de VPC aprimorado
- [Redshift.10] Os clusters do Redshift devem ser criptografados em repouso
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.8] Os buckets de uso geral do S3 devem bloquear o acesso público
- [S3.15] Os buckets de uso geral do S3 devem ter o Object Lock ativado
- [S3.17] Os buckets de uso geral do S3 devem ser criptografados em repouso com AWS KMS keys
- [SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet

- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [SecretsManager.1] Os segredos do Secrets Manager devem ter a rotação automática ativada
- [SecretsManager.2] Os segredos do Secrets Manager configurados com rotação automática devem girar com sucesso
- [SecretsManager.3] Remover segredos não utilizados do Secrets Manager
- [SecretsManager.4] Os segredos do Secrets Manager devem ser alternados dentro de um determinado número de dias
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [SNS.1] Os tópicos do SNS devem ser criptografados em repouso usando AWS KMS
- [PCI.SSM.1] As instâncias do Amazon EC2 gerenciadas pelo devem ter um status de conformidade de patch de COMPLIANT (Em conformidade) após a instalação do patch
- PCI.SSM.2 As instâncias de Amazon EC2 gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.3] Os grupos de regras regionais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras
- [WAF.10] as ACLs AWS WAF da web devem ter pelo menos uma regra ou grupo de regras
- [WAF.11] O registro de ACL AWS WAF da web deve estar ativado

Ásia-Pacífico (Seul)

Os controles a seguir não são compatíveis na Ásia-Pacífico (Seul).

- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado

- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados

- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

Ásia-Pacífico (Singapura)

Os controles a seguir não são compatíveis na Ásia-Pacífico (Singapura).

- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3

- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra

- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

Ásia-Pacífico (Sydney)

Os controles a seguir não são compatíveis na Ásia-Pacífico (Sydney).

- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups

- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

Ásia-Pacífico (Tóquio)

Os controles a seguir não são compatíveis na Ásia-Pacífico (Tóquio).

- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado

- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1

- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

Canadá (Central)

Os controles a seguir não são compatíveis no Canadá (Central).

- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada

- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

China (Pequim)

Os controles a seguir não são compatíveis na China (Pequim).

- Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- [ACM.3] Os certificados ACM devem ser marcados
- [A conta.2] Contas da AWS deve fazer parte de uma organização AWS Organizations
- Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end
- Os estágios da API REST de Gateway devem ter o rastreamento AWS X-Ray habilitado.
- O API Gateway deve ser associado a uma WAF Web ACL
- [AppSync.4] As APIs AWS AppSync do GraphQL devem ser marcadas
- [Athena.2] Os catálogos de dados do Athena devem ser marcados
- [Athena.3] Os grupos de trabalho do Athena devem ser marcados
- [AutoScaling.10] Os grupos do EC2 Auto Scaling devem ser marcados
- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.2] os pontos de AWS Backup recuperação devem ser marcados
- [Backup.3] os AWS Backup cofres devem ser marcados
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [Backup.5] os planos de AWS Backup backup devem ser marcados
- [CloudFormation.2] as CloudFormation pilhas devem ser marcadas
- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS

- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CloudTrail.9] CloudTrail trilhas devem ser marcadas
- [CloudWatch.15] CloudWatch os alarmes devem ter ações especificadas configuradas
- [CloudWatch.16] os grupos de CloudWatch registros devem ser mantidos por um período de tempo especificado
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [Detetive.1] Os gráficos do comportamento do detetive devem ser marcados
- [DMS.2] Os certificados DMS devem ser marcados
- [DMS.3] As assinaturas de eventos do DMS devem ser marcadas
- [DMS.4] As instâncias de replicação do DMS devem ser marcadas
- [DMS.5] Os grupos de sub-redes de replicação do DMS devem ser marcados
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos
- [DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch
- Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- As tabelas do DynamoDB devem estar presentes em um plano de backup
- [DynamoDB.5] As tabelas do DynamoDB devem ser marcadas
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito

- As sub-redes do Amazon EC2 não devem atribuir automaticamente endereços IP públicos
- As listas de controle de acesso à rede não utilizadas devem ser removidas
- [EC2.20] Ambos os túneis VPN para uma conexão VPN Site-to-Site devem estar ativos AWS
- [PCI.EC2.3] Os grupos de segurança do Amazon EC2 devem ser removidos
- Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.33] Os anexos do gateway de trânsito EC2 devem ser marcados
- [EC2.34] As tabelas de rotas do gateway de trânsito EC2 devem ser marcadas
- [EC2.35] As interfaces de rede EC2 devem ser marcadas
- [EC2.36] Os gateways de clientes do EC2 devem ser marcados
- [EC2.37] Os endereços IP elásticos do EC2 devem ser marcados
- [EC2.38] As instâncias do EC2 devem ser marcadas
- [EC2.39] Os gateways de internet EC2 devem ser marcados
- [EC2.40] Os gateways NAT EC2 devem ser marcados
- [EC2.41] As ACLs de rede EC2 devem ser marcadas
- [EC2.42] As tabelas de rotas do EC2 devem ser marcadas
- [EC2.43] Grupos de segurança do EC2 devem ser marcados
- [EC2.44] As sub-redes do EC2 devem ser marcadas
- [EC2.45] Os volumes do EC2 devem ser marcados
- [EC2.46] Amazon VPCs devem ser marcadas
- [EC2.47] Os serviços de endpoint da Amazon VPC devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.49] As conexões de emparelhamento da Amazon VPC devem ser marcadas
- [EC2.50] Os gateways de VPN EC2 devem ser marcados
- [EC2.51] Os endpoints da Client VPN do EC2 devem ter o registro em log de conexão do cliente habilitado
- [EC2.52] Os gateways de trânsito do EC2 devem ser marcados
- [EC2.53] Os grupos de segurança do EC2 não devem permitir a entrada de 0.0.0.0/0 nas portas de administração remota do servidor
- [EC2.54] Os grupos de segurança do EC2 não devem permitir a entrada de: :/0 nas portas de administração do servidor remoto

- Os repositórios privados do ECR devem ter a digitalização de imagens configurada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário.
- [ECS.13] Os serviços do ECS devem ser marcados
- [ECS.14] Os clusters ECS devem ser marcados
- [ECS.15] As definições de tarefas do ECS devem ser marcadas
- [EFS.5] Os pontos de acesso do EFS devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [EKS.6] Os clusters EKS devem ser marcados
- [EKS.7] As configurações do provedor de identidade EKS devem ser marcadas
- [ELB.2] Os balanceadores de carga clássicos com ouvintes SSL/HTTPS devem usar um certificado fornecido pelo AWS Certificate Manager
- [ELB.16] Os balanceadores de carga de aplicativos devem ser associados a uma ACL da web AWS WAF
- [ElastiCache.1] Os clusters ElastiCache Redis devem ter o backup automático ativado
- [ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de integridade aprimorados habilitados
- [ElasticBeanstalk.2] As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas
- [ElasticBeanstalk.3] O Elastic Beanstalk deve transmitir registros para CloudWatch
- [EMR.2] A configuração de bloqueio de acesso público do Amazon EMR deve estar habilitada
- Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós
- [ES.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado
- [ES.9] Os domínios do Elasticsearch devem ser marcados
- [EventBridge.2] ônibus de EventBridge eventos devem ser etiquetados
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups

- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- Os AWS Glue trabalhos [Glue.1] devem ser marcados
- [GuardDuty.1] GuardDuty deve ser ativado
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] Os GuardDuty IPsets devem ser marcados
- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.23] Os analisadores do IAM Access Analyzer devem ser marcados
- [IAM.24] As funções do IAM devem ser marcadas
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloudShellFullAccess
- [IAM.28] O analisador de acesso externo do IAM Access Analyzer deve estar ativado
- [IoT.1] perfis de AWS IoT Core segurança devem ser marcados
- [IoT.2] as ações de AWS IoT Core mitigação devem ser marcadas
- [IoT.3] as AWS IoT Core dimensões devem ser marcadas
- [IoT.4] os AWS IoT Core autorizadores devem ser marcados
- [IoT.5] aliases de AWS IoT Core função devem ser marcados
- As AWS IoT Core políticas [IoT.6] devem ser marcadas
- [Kinesis.2] Os streams do Kinesis devem ser marcados
- [Lambda.6] As funções Lambda devem ser marcadas
- [Macie.1] O Amazon Macie deve estar ativado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve ser ativada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- [MQ.4] Os corretores do Amazon MQ devem ser marcados
- Os clusters de banco de dados Neptune devem ser criptografados em repouso

- [Neptune.2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch
- Os instantâneos do cluster de banco de dados Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- Os clusters de banco de dados Neptune devem ter backups automatizados habilitados
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.7] Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- [Neptune.9] Os clusters de banco de dados do Neptune devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.1] Os firewalls do Network Firewall devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.2] O registro do Firewall de Rede deve estar ativado
- [NetworkFirewall.3] As políticas de Firewall de Rede devem ter pelo menos um grupo de regras associado
- [NetworkFirewall.4] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar pacotes completos
- [NetworkFirewall.5] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar para pacotes fragmentados
- [NetworkFirewall.6] O grupo de regras do Stateless Network Firewall não deve estar vazio
- [NetworkFirewall.7] Os firewalls do Firewall de Rede devem ser marcados
- [NetworkFirewall.8] As políticas de firewall do Network Firewall devem ser marcadas
- [NetworkFirewall.9] Os firewalls do Firewall de Rede devem ter a proteção contra exclusão ativada
- Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada
- Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público
- Os OpenSearch domínios [Opensearch.3] devem criptografar os dados enviados entre os nós
- O registro de erros de OpenSearch domínio [Opensearch.4] nos CloudWatch registros deve estar ativado
- Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado
- Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados

- Os OpenSearch domínios [Opensearch.7] devem ter um controle de acesso refinado ativado
- [Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente
- Os OpenSearch domínios [Opensearch.9] devem ser marcados
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [PCA.1] a autoridade de certificação AWS Private CA raiz deve ser desativada
- [RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada
- A autenticação do IAM deve ser configurada para instâncias do RDS
- A autenticação do IAM deve ser configurada para instâncias do RDS
- [RDS.13] As atualizações automáticas de versões secundárias do RDS devem ser ativadas
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.15] Os clusters de banco de dados do RDS devem ser configurados para várias zonas de disponibilidade
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [RDS.28] Os clusters de banco de dados do RDS devem ser marcados
- [RDS.29] Os instantâneos do cluster de banco de dados do RDS devem ser marcados
- [RDS.30] As instâncias de banco de dados do RDS devem ser marcadas
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [RDS.32] Os instantâneos do banco de dados do RDS devem ser marcados
- [RDS.33] Os grupos de sub-redes do banco de dados do RDS devem ser marcados
- [RDS.34] Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch
- Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- Os clusters do Redshift devem usar roteamento de VPC aprimorado

- [Redshift.10] Os clusters do Redshift devem ser criptografados em repouso
- [Redshift.11] Os clusters do Redshift devem ser marcados
- [Redshift.12] As assinaturas de notificação de eventos do Redshift devem ser marcadas
- [Redshift.13] Os instantâneos do cluster do Redshift devem ser marcados
- [Redshift.14] Os grupos de sub-redes do cluster Redshift devem ser marcados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas
- [S3.8] Os buckets de uso geral do S3 devem bloquear o acesso público
- [S3.14] Os buckets de uso geral do S3 devem ter o controle de versão ativado
- [S3.22] Os buckets de uso geral do S3 devem registrar eventos de gravação em nível de objeto
- [S3.23] Os buckets de uso geral do S3 devem registrar eventos de leitura em nível de objeto
- [SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [SES.1] As listas de contatos do SES devem ser marcadas
- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [SecretsManager.3] Remover segredos não utilizados do Secrets Manager
- [SecretsManager.4] Os segredos do Secrets Manager devem ser alternados dentro de um determinado número de dias
- [SecretsManager.5] Os segredos do Secrets Manager devem ser marcados
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [SNS.3] Os tópicos do SNS devem ser marcados
- [SQS.2] As filas SQS devem ser marcadas
- [StepFunctions.2] As atividades do Step Functions devem ser marcadas
- Os AWS Transfer Family fluxos de trabalho [Transfer.1] devem ser marcados

- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.3] Os grupos de regras regionais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras
- [WAF.11] O registro de ACL AWS WAF da web deve estar ativado

China (Ningxia)

Os controles a seguir não são compatíveis na China (Ningxia).

- Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- [ACM.3] Os certificados ACM devem ser marcados
- [A conta.2] Contas da AWS deve fazer parte de uma organização AWS Organizations
- Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end
- Os estágios da API REST de Gateway devem ter o rastreamento AWS X-Ray habilitado.
- O API Gateway deve ser associado a uma WAF Web ACL
- [AppSync.4] As APIs AWS AppSync do GraphQL devem ser marcadas
- [Athena.2] Os catálogos de dados do Athena devem ser marcados
- [Athena.3] Os grupos de trabalho do Athena devem ser marcados
- [AutoScaling.10] Os grupos do EC2 Auto Scaling devem ser marcados
- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.2] os pontos de AWS Backup recuperação devem ser marcados
- [Backup.3] os AWS Backup cofres devem ser marcados
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados

- [Backup.5] os planos de AWS Backup backup devem ser marcados
- [CloudFormation.2] as CloudFormation pilhas devem ser marcadas
- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CloudTrail.9] CloudTrail trilhas devem ser marcadas
- [CloudWatch.15] CloudWatch os alarmes devem ter ações especificadas configuradas
- [CloudWatch.16] os grupos de CloudWatch registros devem ser mantidos por um período de tempo especificado
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [Detetive.1] Os gráficos do comportamento do detetive devem ser marcados
- [DMS.2] Os certificados DMS devem ser marcados
- [DMS.3] As assinaturas de eventos do DMS devem ser marcadas
- [DMS.4] As instâncias de replicação do DMS devem ser marcadas
- [DMS.5] Os grupos de sub-redes de replicação do DMS devem ser marcados
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado

- Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- As tabelas do DynamoDB devem estar presentes em um plano de backup
- [DynamoDB.5] As tabelas do DynamoDB devem ser marcadas
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- As sub-redes do Amazon EC2 não devem atribuir automaticamente endereços IP públicos
- As listas de controle de acesso à rede não utilizadas devem ser removidas
- [EC2.20] Ambos os túneis VPN para uma conexão VPN Site-to-Site devem estar ativos AWS
- [PCI.EC2.3] Os grupos de segurança do Amazon EC2 devem ser removidos
- Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.33] Os anexos do gateway de trânsito EC2 devem ser marcados
- [EC2.34] As tabelas de rotas do gateway de trânsito EC2 devem ser marcadas
- [EC2.35] As interfaces de rede EC2 devem ser marcadas
- [EC2.36] Os gateways de clientes do EC2 devem ser marcados
- [EC2.37] Os endereços IP elásticos do EC2 devem ser marcados
- [EC2.38] As instâncias do EC2 devem ser marcadas
- [EC2.39] Os gateways de internet EC2 devem ser marcados
- [EC2.40] Os gateways NAT EC2 devem ser marcados
- [EC2.41] As ACLs de rede EC2 devem ser marcadas
- [EC2.42] As tabelas de rotas do EC2 devem ser marcadas
- [EC2.43] Grupos de segurança do EC2 devem ser marcados
- [EC2.44] As sub-redes do EC2 devem ser marcadas
- [EC2.45] Os volumes do EC2 devem ser marcados
- [EC2.46] Amazon VPCs devem ser marcadas
- [EC2.47] Os serviços de endpoint da Amazon VPC devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.49] As conexões de emparelhamento da Amazon VPC devem ser marcadas
- [EC2.50] Os gateways de VPN EC2 devem ser marcados

- [EC2.51] Os endpoints da Client VPN do EC2 devem ter o registro em log de conexão do cliente habilitado
- [EC2.52] Os gateways de trânsito do EC2 devem ser marcados
- Os repositórios privados do ECR devem ter a digitalização de imagens configurada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário.
- [ECS.13] Os serviços do ECS devem ser marcados
- [ECS.14] Os clusters ECS devem ser marcados
- [ECS.15] As definições de tarefas do ECS devem ser marcadas
- Os pontos de acesso do EFS devem impor um diretório raiz
- Os pontos de acesso do EFS devem impor uma identidade de usuário
- [EFS.5] Os pontos de acesso do EFS devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [EKS.6] Os clusters EKS devem ser marcados
- [EKS.7] As configurações do provedor de identidade EKS devem ser marcadas
- [ELB.2] Os balanceadores de carga clássicos com ouvintes SSL/HTTPS devem usar um certificado fornecido pelo AWS Certificate Manager
- [ELB.16] Os balanceadores de carga de aplicativos devem ser associados a uma ACL da web AWS WAF
- [ElastiCache.1] Os clusters ElastiCache Redis devem ter o backup automático ativado
- [ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de integridade aprimorados habilitados
- [ElasticBeanstalk.2] As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas
- [ElasticBeanstalk.3] O Elastic Beanstalk deve transmitir registros para CloudWatch
- [EMR.2] A configuração de bloqueio de acesso público do Amazon EMR deve estar habilitada
- [ES.1] Os domínios do devem ter a criptografia em repouso habilitada.
- Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós
- [ES.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado

- [ES.9] Os domínios do Elasticsearch devem ser marcados
- [EventBridge.2] ônibus de EventBridge eventos devem ser etiquetados
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- Os AWS Glue trabalhos [Glue.1] devem ser marcados
- [GuardDuty.1] GuardDuty deve ser ativado
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] Os GuardDuty IPsets devem ser marcados
- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.23] Os analisadores do IAM Access Analyzer devem ser marcados
- [IAM.24] As funções do IAM devem ser marcadas
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloudShellFullAccess
- [IAM.28] O analisador de acesso externo do IAM Access Analyzer deve estar ativado
- [IoT.1] perfis de AWS IoT Core segurança devem ser marcados
- [IoT.2] as ações de AWS IoT Core mitigação devem ser marcadas
- [IoT.3] as AWS IoT Core dimensões devem ser marcadas
- [IoT.4] os AWS IoT Core autorizadores devem ser marcados
- [IoT.5] aliases de AWS IoT Core função devem ser marcados
- As AWS IoT Core políticas [IoT.6] devem ser marcadas
- [Kinesis.2] Os streams do Kinesis devem ser marcados
- [PCI.lambda.1] As funções do devem proibir o acesso público

- [Lambda.2] As funções do devem usar os tempos de execução mais recentes
- [PCI.Lambda.2] As funções do Lambda devem estar em uma VPC
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- [Lambda.6] As funções Lambda devem ser marcadas
- [Macie.1] O Amazon Macie deve estar ativado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve ser ativada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- [MQ.4] Os corretores do Amazon MQ devem ser marcados
- Os instantâneos do cluster de banco de dados Neptune não devem ser públicos
- [NetworkFirewall.1] Os firewalls do Network Firewall devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.2] O registro do Firewall de Rede deve estar ativado
- [NetworkFirewall.3] As políticas de Firewall de Rede devem ter pelo menos um grupo de regras associado
- [NetworkFirewall.4] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar pacotes completos
- [NetworkFirewall.5] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar para pacotes fragmentados
- [NetworkFirewall.6] O grupo de regras do Stateless Network Firewall não deve estar vazio
- [NetworkFirewall.7] Os firewalls do Firewall de Rede devem ser marcados
- [NetworkFirewall.8] As políticas de firewall do Network Firewall devem ser marcadas
- [NetworkFirewall.9] Os firewalls do Firewall de Rede devem ter a proteção contra exclusão ativada
- Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada
- Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público
- Os OpenSearch domínios [Opensearch.3] devem criptografar os dados enviados entre os nós
- O registro de erros de OpenSearch domínio [Opensearch.4] nos CloudWatch registros deve estar ativado
- Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado
- Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados

- Os OpenSearch domínios [Opensearch.7] devem ter um controle de acesso refinado ativado
- [Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente
- Os OpenSearch domínios [Opensearch.9] devem ser marcados
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [PCA.1] a autoridade de certificação AWS Private CA raiz deve ser desativada
- [RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada
- [RDS.9] As instâncias de banco de dados do RDS devem publicar registros no Logs CloudWatch
- A autenticação do IAM deve ser configurada para instâncias do RDS
- A autenticação do IAM deve ser configurada para instâncias do RDS
- [RDS.13] As atualizações automáticas de versões secundárias do RDS devem ser ativadas
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.15] Os clusters de banco de dados do RDS devem ser configurados para várias zonas de disponibilidade
- Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- [RDS.28] Os clusters de banco de dados do RDS devem ser marcados
- [RDS.29] Os instantâneos do cluster de banco de dados do RDS devem ser marcados
- [RDS.30] As instâncias de banco de dados do RDS devem ser marcadas
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [RDS.32] Os instantâneos do banco de dados do RDS devem ser marcados
- [RDS.33] Os grupos de sub-redes do banco de dados do RDS devem ser marcados
- [RDS.34] Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch
- Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados
- Os clusters do Redshift devem usar roteamento de VPC aprimorado

- [Redshift.10] Os clusters do Redshift devem ser criptografados em repouso
- [Redshift.11] Os clusters do Redshift devem ser marcados
- [Redshift.12] As assinaturas de notificação de eventos do Redshift devem ser marcadas
- [Redshift.13] Os instantâneos do cluster do Redshift devem ser marcados
- [Redshift.14] Os grupos de sub-redes do cluster Redshift devem ser marcados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas
- [S3.8] Os buckets de uso geral do S3 devem bloquear o acesso público
- [S3.14] Os buckets de uso geral do S3 devem ter o controle de versão ativado
- [SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [SES.1] As listas de contatos do SES devem ser marcadas
- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [SecretsManager.3] Remover segredos não utilizados do Secrets Manager
- [SecretsManager.4] Os segredos do Secrets Manager devem ser alternados dentro de um determinado número de dias
- [SecretsManager.5] Os segredos do Secrets Manager devem ser marcados
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [SNS.3] Os tópicos do SNS devem ser marcados
- [SQS.2] As filas SQS devem ser marcadas
- [StepFunctions.2] As atividades do Step Functions devem ser marcadas
- Os AWS Transfer Family fluxos de trabalho [Transfer.1] devem ser marcados
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado

- [WAF.3] Os grupos de regras regionais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras
- [WAF.11] O registro de ACL AWS WAF da web deve estar ativado

Europa (Frankfurt)

Os controles a seguir não são compatíveis na Europa (Frankfurt).

- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado

- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

Europa (Irlanda)

Os controles a seguir não são compatíveis na Europa (Irlanda).

- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes

- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

Europa (Londres)

Os controles a seguir não são compatíveis na Europa (Londres).

- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado

- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas

- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

Europa (Milão)

Os controles a seguir não são compatíveis na Europa (Milão).

- Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- [ApiGateway.1] O REST do API Gateway WebSocket e o registro de execução da API devem estar habilitados
- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3

- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais
- [CodeBuild.2] as variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- As instâncias de replicação do PCI.DMS.1 Database Migration Service não devem ser públicas
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- [EC2.3] Os volumes anexados do Amazon EBS devem ser criptografados em repouso.
- As instâncias EC2 interrompidas devem ser removidas após um período de tempo especificado
- As instâncias do EC2 devem usar o Instance Metadata Service Version 2 (IMDSv2)
- [PCI.EC2.4] Os EIPs do EC2 não utilizados devem ser removidos
- [EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22
- [EC2.14] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 3389
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- Os clusters do ECS devem usar Container Insights
- [EFS.1] O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS
- [EFS.2] Os volumes do Amazon EFS devem estar em planos de backup
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- Os endpoints do cluster EKS não devem ser acessíveis ao público
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [ELBv2.1] O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS

- [ELB.2] Os balanceadores de carga clássicos com ouvintes SSL/HTTPS devem usar um certificado fornecido pelo AWS Certificate Manager
- O Application Load Balancer deve ser configurado para eliminar cabeçalhos http
- [ELB.8] Os balanceadores de carga clássicos com ouvintes SSL devem usar uma política de segurança predefinida que tenha uma duração forte AWS Config
- [ELB.16] Os balanceadores de carga de aplicativos devem ser associados a uma ACL da web AWS WAF
- [EMR.1] Os nós primários do cluster do Amazon EMR não devem ter endereços IP públicos
- Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [GuardDuty.1] GuardDuty deve ser ativado
- [IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos
- [IAM.18] Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [IoT.1] perfis de AWS IoT Core segurança devem ser marcados
- [IoT.2] as ações de AWS IoT Core mitigação devem ser marcadas
- [IoT.3] as AWS IoT Core dimensões devem ser marcadas
- [IoT.4] os AWS IoT Core autorizadores devem ser marcados
- [IoT.5] aliases de AWS IoT Core função devem ser marcados
- As AWS IoT Core políticas [IoT.6] devem ser marcadas
- [KMS.3] não AWS KMS keys deve ser excluído acidentalmente
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os clusters de banco de dados Neptune devem ser criptografados em repouso

- [Neptune.2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch
- Os instantâneos do cluster de banco de dados Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- Os clusters de banco de dados Neptune devem ter backups automatizados habilitados
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.7] Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- [Neptune.9] Os clusters de banco de dados do Neptune devem ser implantados em várias zonas de disponibilidade
- Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada
- Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público
- Os OpenSearch domínios [Opensearch.3] devem criptografar os dados enviados entre os nós
- O registro de erros de OpenSearch domínio [Opensearch.4] nos CloudWatch registros deve estar ativado
- Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado
- Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados
- Os OpenSearch domínios [Opensearch.7] devem ter um controle de acesso refinado ativado
- [Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [RDS.1] Os instantâneos do RDS devem ser privados
- Os instantâneos do cluster do RDS e os instantâneos do banco de dados devem ser criptografados em repouso
- [RDS.9] As instâncias de banco de dados do RDS devem publicar registros no Logs CloudWatch
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito
- Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados

- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [PCI.SSM.1] As instâncias do Amazon EC2 gerenciadas pelo devem ter um status de conformidade de patch de COMPLIANT (Em conformidade) após a instalação do patch
- PCI.SSM.2 As instâncias de Amazon EC2 gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras
- [WAF.11] O registro de ACL AWS WAF da web deve estar ativado

Europa (Paris)

Os controles a seguir não são compatíveis na Europa (Paris).

- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados

- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas

- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

Europa (Espanha)

Os controles a seguir não são compatíveis na Europa (Espanha).

- Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- [A conta.2] Contas da AWS deve fazer parte de uma organização AWS Organizations
- [ApiGateway.1] O REST do API Gateway WebSocket e o registro de execução da API devem estar habilitados
- Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end
- Os estágios da API REST de Gateway devem ter o rastreamento AWS X-Ray habilitado.
- O API Gateway deve ser associado a uma WAF Web ACL
- As rotas do API de Gateway devem especificar um tipo de autorização
- O registro de acesso deve ser configurado para os estágios V2 do API de Gateway
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado
- [AppSync.5] As APIs AWS AppSync do GraphQL não devem ser autenticadas com chaves de API
- [Athena.2] Os catálogos de dados do Athena devem ser marcados

- [Athena.3] Os grupos de trabalho do Athena devem ser marcados
- [AutoScaling.1] Grupos de Auto Scaling associados a um balanceador de carga devem usar verificações de integridade do ELB
- As instâncias do Amazon EC2 lançadas usando as configurações de execução em grupo do Auto Scaling não devem ter endereços IP públicos
- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.2] os pontos de AWS Backup recuperação devem ser marcados
- [Backup.3] os AWS Backup cofres devem ser marcados
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [Backup.5] os planos de AWS Backup backup devem ser marcados
- [CloudFormation.2] as CloudFormation pilhas devem ser marcadas
- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CloudTrail.6] Certifique-se de que o bucket do S3 usado para armazenar CloudTrail registros não esteja acessível ao público
- [CloudTrail.7] Certifique-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrail S3
- [CloudWatch.16] os grupos de CloudWatch registros devem ser mantidos por um período de tempo especificado
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados

- [CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais
- [CodeBuild.2] as variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado
- [CodeBuild.3] Os registros do CodeBuild S3 devem ser criptografados
- [CodeBuild.4] ambientes de CodeBuild projeto devem ter uma duração de registro AWS Config
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [Detetive.1] Os gráficos do comportamento do detetive devem ser marcados
- As instâncias de replicação do PCI.DMS.1 Database Migration Service não devem ser públicas
- [DMS.2] Os certificados DMS devem ser marcados
- [DMS.3] As assinaturas de eventos do DMS devem ser marcadas
- [DMS.4] As instâncias de replicação do DMS devem ser marcadas
- [DMS.5] Os grupos de sub-redes de replicação do DMS devem ser marcados
- As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- Os endpoints do DMS devem usar SSL
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos
- [DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch
- Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- As tabelas do DynamoDB devem escalar automaticamente a capacidade de acordo com a demanda

- [DynamoDB.2] As tabelas do DynamoDB devem ter a recuperação ativada point-in-time
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- As tabelas do DynamoDB devem estar presentes em um plano de backup
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- [PCI.EC2.1] Os instantâneos do Amazon EBS não devem ser restauráveis publicamente
- [EC2.2] O grupo de segurança padrão da VPC não deve permitir o tráfego de entrada e saída
- [EC2.3] Os volumes anexados do Amazon EBS devem ser criptografados em repouso.
- As instâncias EC2 interrompidas devem ser removidas após um período de tempo especificado
- [EC2.6] O registro de fluxo de VPC deve ser ativado em todas as VPCs
- [EC2.7] A criptografia padrão do EBS deve estar ativada
- As instâncias do EC2 devem usar o Instance Metadata Service Version 2 (IMDSv2)
- As instâncias do Amazon EC2 não devem ter um endereço IPv4 público
- O Amazon EC2 deve ser configurado para usar endpoints da VPC criados para o serviço Amazon EC2
- [EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22
- [EC2.14] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 3389
- As sub-redes do Amazon EC2 não devem atribuir automaticamente endereços IP públicos
- As listas de controle de acesso à rede não utilizadas devem ser removidas
- As instâncias do Amazon EC2 não devem usar vários ENIs
- Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas
- [EC2.20] Ambos os túneis VPN para uma conexão VPN Site-to-Site devem estar ativos AWS
- [PCI.EC2.3] Os grupos de segurança do Amazon EC2 devem ser removidos
- Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- Os modelos de lançamento do Amazon EC2 não devem atribuir IPs públicos às interfaces de rede
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.34] As tabelas de rotas do gateway de trânsito EC2 devem ser marcadas
- [EC2.40] Os gateways NAT EC2 devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.51] Os endpoints da Client VPN do EC2 devem ter o registro em log de conexão do cliente habilitado

- Os repositórios privados do ECR devem ter a digitalização de imagens configurada
- [ECR.2] Os repositórios privados do ECR devem ter a imutabilidade da tag configurada
- Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário.
- As definições de tarefas do ECS devem ter uma configuração de registro em log
- [EFS.1] O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS
- [EFS.2] Os volumes do Amazon EFS devem estar em planos de backup
- Os pontos de acesso do EFS devem impor um diretório raiz
- Os pontos de acesso do EFS devem impor uma identidade de usuário
- [EFS.5] Os pontos de acesso do EFS devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- Os endpoints do cluster EKS não devem ser acessíveis ao público
- Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [ELBv2.1] O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS
- [ELB.2] Os balanceadores de carga clássicos com ouvintes SSL/HTTPS devem usar um certificado fornecido pelo AWS Certificate Manager
- Os receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS
- O Application Load Balancer deve ser configurado para eliminar cabeçalhos http
- O registro em log do Classic Load Balancer e Application Load Balancer deve estar ativado
- [ELB.6] Os balanceadores de carga de aplicativos, gateways e redes devem ter a proteção contra exclusão ativada
- [ELB.8] Os balanceadores de carga clássicos com ouvintes SSL devem usar uma política de segurança predefinida que tenha uma duração forte AWS Config
- Os Classic Load Balancers devem ter o balanceador de carga entre zonas habilitado
- O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso

- [ELB.16] Os balanceadores de carga de aplicativos devem ser associados a uma ACL da web AWS WAF
- [ElastiCache.1] Os clusters ElastiCache Redis devem ter o backup automático ativado
- [ElastiCache.6] ElastiCache para grupos de replicação do Redis antes da versão 6.0 deve usar o Redis AUTH
- [ElastiCache.7] os ElastiCache clusters não devem usar o grupo de sub-rede padrão
- [ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de integridade aprimorados habilitados
- [ElasticBeanstalk.2] As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas
- [ElasticBeanstalk.3] O Elastic Beanstalk deve transmitir registros para CloudWatch
- [EMR.1] Os nós primários do cluster do Amazon EMR não devem ter endereços IP públicos
- [ES.1] Os domínios do devem ter a criptografia em repouso habilitada.
- [ES.2] Os domínios do Elasticsearch não devem ser publicamente acessíveis
- Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós
- [ES.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado
- [EventBridge.2] ônibus de EventBridge eventos devem ser etiquetados
- [EventBridge.3] os ônibus de eventos EventBridge personalizados devem ter uma política baseada em recursos anexada
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- Os AWS Glue trabalhos [Glue.1] devem ser marcados
- [GuardDuty.1] GuardDuty deve ser ativado
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] Os GuardDuty IPsets devem ser marcados
- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [IAM.1] As políticas do não devem permitir privilégios administrativos completos "*"

- [IAM.2] Os usuários do não devem ter políticas do IAM anexadas
- [IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos
- [IAM.4] A chave de acesso do usuário raiz do não deve existir
- [IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console
- As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.18] Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support
- [PCI.IAM.6] A MFA deve estar habilitada para todos os usuários do
- As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.24] As funções do IAM devem ser marcadas
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloudShellFullAccess
- [IoT.1] perfis de AWS IoT Core segurança devem ser marcados
- [IoT.2] as ações de AWS IoT Core mitigação devem ser marcadas
- [IoT.3] as AWS IoT Core dimensões devem ser marcadas
- [IoT.4] os AWS IoT Core autorizadores devem ser marcados
- [IoT.5] aliases de AWS IoT Core função devem ser marcados
- As AWS IoT Core políticas [IoT.6] devem ser marcadas
- Os fluxos do Kinesis devem ser criptografados em repouso
- As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS
- A rotação de AWS KMS teclas [KMS.4] deve estar ativada
- [PCI.lambda.1] As funções do devem proibir o acesso público
- [Lambda.2] As funções do devem usar os tempos de execução mais recentes
- [PCI.Lambda.2] As funções do Lambda devem estar em uma VPC
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade

- [Macie.1] O Amazon Macie deve estar ativado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve ser ativada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- [MQ.4] Os corretores do Amazon MQ devem ser marcados
- Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- [MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch
- Os instantâneos do cluster de banco de dados Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- Os clusters de banco de dados Neptune devem ter backups automatizados habilitados
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.7] Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- [Neptune.9] Os clusters de banco de dados do Neptune devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.1] Os firewalls do Network Firewall devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.2] O registro do Firewall de Rede deve estar ativado
- [NetworkFirewall.3] As políticas de Firewall de Rede devem ter pelo menos um grupo de regras associado
- [NetworkFirewall.4] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar pacotes completos
- [NetworkFirewall.5] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar para pacotes fragmentados

- [NetworkFirewall.6] O grupo de regras do Stateless Network Firewall não deve estar vazio
- [NetworkFirewall.9] Os firewalls do Firewall de Rede devem ter a proteção contra exclusão ativada
- Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada
- Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público
- Os OpenSearch domínios [Opensearch.3] devem criptografar os dados enviados entre os nós
- O registro de erros de OpenSearch domínio [Opensearch.4] nos CloudWatch registros deve estar ativado
- Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado
- Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados
- Os OpenSearch domínios [Opensearch.7] devem ter um controle de acesso refinado ativado
- [Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente
- Os OpenSearch domínios [Opensearch.9] devem ser marcados
- Os OpenSearch domínios [Opensearch.10] devem ter a atualização de software mais recente instalada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [RDS.1] Os instantâneos do RDS devem ser privados
- [RDS.2] As instâncias de banco de dados do RDS devem proibir o acesso público, conforme determinado pela duração PubliclyAccessible AWS Config
- [RDS.3] As instâncias de banco de dados do RDS devem ter a criptografia em repouso habilitada.
- Os instantâneos do cluster do RDS e os instantâneos do banco de dados devem ser criptografados em repouso
- As instâncias de banco de dados do RDS devem ser configuradas com várias zonas de disponibilidade
- O monitoramento aprimorado deve ser configurado para instâncias de banco de dados do RDS
- [RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada
- [RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada
- [RDS.9] As instâncias de banco de dados do RDS devem publicar registros no Logs CloudWatch
- A autenticação do IAM deve ser configurada para instâncias do RDS
- As instâncias do RDS devem ter backups automáticos habilitados
- A autenticação do IAM deve ser configurada para instâncias do RDS

- [RDS.13] As atualizações automáticas de versões secundárias do RDS devem ser ativadas
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.15] Os clusters de banco de dados do RDS devem ser configurados para várias zonas de disponibilidade
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [RDS.28] Os clusters de banco de dados do RDS devem ser marcados
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [RDS.34] Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch
- Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [PCI.Redshift.1] Os clusters do devem proibir o acesso público
- As conexões com os clusters do Amazon Redshift devem ser criptografadas em trânsito
- Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados
- O Amazon Redshift deve ter as atualizações automáticas para as versões principais habilitadas
- Os clusters do Redshift devem usar roteamento de VPC aprimorado
- [Redshift.10] Os clusters do Redshift devem ser criptografados em repouso
- [Redshift.12] As assinaturas de notificação de eventos do Redshift devem ser marcadas
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas
- [S3.5] Os buckets de uso geral do S3 devem exigir solicitações de uso de SSL
- [S3.6] As políticas de bucket de uso geral do S3 devem restringir o acesso a outros Contas da AWS

- [S3.8] Os buckets de uso geral do S3 devem bloquear o acesso público
- [S3.9] Os buckets de uso geral do S3 devem ter o registro de acesso ao servidor ativado
- [S3.15] Os buckets de uso geral do S3 devem ter o Object Lock ativado
- [S3.17] Os buckets de uso geral do S3 devem ser criptografados em repouso com AWS KMS keys
- [SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet
- [SageMaker.2] as instâncias do SageMaker notebook devem ser iniciadas em uma VPC personalizada
- [SageMaker.3] Os usuários não devem ter acesso root às instâncias do SageMaker notebook
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [SES.1] As listas de contatos do SES devem ser marcadas
- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [SecretsManager.2] Os segredos do Secrets Manager configurados com rotação automática devem girar com sucesso
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [SNS.1] Os tópicos do SNS devem ser criptografados em repouso usando AWS KMS
- [SNS.3] Os tópicos do SNS devem ser marcados
- As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas SQS devem ser marcadas
- [SSM.1] As instâncias do Amazon EC2 devem ser gerenciadas por AWS Systems Manager
- [PCI.SSM.1] As instâncias do Amazon EC2 gerenciadas pelo devem ter um status de conformidade de patch de COMPLIANT (Em conformidade) após a instalação do patch
- PCI.SSM.2 As instâncias de Amazon EC2 gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [StepFunctions.1] As máquinas de estado do Step Functions devem ter o registro ativado
- Os AWS Transfer Family fluxos de trabalho [Transfer.1] devem ser marcados
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.2] As regras regionais AWS WAF clássicas devem ter pelo menos uma condição

- [WAF.3] Os grupos de regras regionais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.4] As ACLs regionais AWS WAF clássicas da web devem ter pelo menos uma regra ou grupo de regras
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras
- [WAF.10] as ACLs AWS WAF da web devem ter pelo menos uma regra ou grupo de regras
- [WAF.11] O registro de ACL AWS WAF da web deve estar ativado

Europa (Estocolmo)

Os controles a seguir não são compatíveis na Europa (Estocolmo).

- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado

- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos
- [DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch
- Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS

- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

Europa (Zurique)

Os controles a seguir não são compatíveis na Europa (Zurique).

- Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- [ApiGateway.1] O REST do API Gateway WebSocket e o registro de execução da API devem estar habilitados
- Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end
- As rotas do API de Gateway devem especificar um tipo de autorização
- O registro de acesso deve ser configurado para os estágios V2 do API de Gateway
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado
- [AppSync.5] As APIs AWS AppSync do GraphQL não devem ser autenticadas com chaves de API
- [Athena.2] Os catálogos de dados do Athena devem ser marcados
- [Athena.3] Os grupos de trabalho do Athena devem ser marcados
- [AutoScaling.1] Grupos de Auto Scaling associados a um balanceador de carga devem usar verificações de integridade do ELB
- As instâncias do Amazon EC2 lançadas usando as configurações de execução em grupo do Auto Scaling não devem ter endereços IP públicos
- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.2] os pontos de AWS Backup recuperação devem ser marcados
- [Backup.3] os AWS Backup cofres devem ser marcados

- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [Backup.5] os planos de AWS Backup backup devem ser marcados
- [CloudFormation.2] as CloudFormation pilhas devem ser marcadas
- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CloudTrail.6] Certifique-se de que o bucket do S3 usado para armazenar CloudTrail registros não esteja acessível ao público
- [CloudTrail.7] Certifique-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrail S3
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais
- [CodeBuild.2] as variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado
- [CodeBuild.3] Os registros do CodeBuild S3 devem ser criptografados
- [CodeBuild.4] ambientes de CodeBuild projeto devem ter uma duração de registro AWS Config
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [Detetive.1] Os gráficos do comportamento do detetive devem ser marcados
- As instâncias de replicação do PCI.DMS.1 Database Migration Service não devem ser públicas

- [DMS.2] Os certificados DMS devem ser marcados
- [DMS.3] As assinaturas de eventos do DMS devem ser marcadas
- [DMS.4] As instâncias de replicação do DMS devem ser marcadas
- [DMS.5] Os grupos de sub-redes de replicação do DMS devem ser marcados
- As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- Os endpoints do DMS devem usar SSL
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos
- [DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch
- Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- As tabelas do DynamoDB devem escalar automaticamente a capacidade de acordo com a demanda
- [DynamoDB.2] As tabelas do DynamoDB devem ter a recuperação ativada point-in-time
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- As tabelas do DynamoDB devem estar presentes em um plano de backup
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- [EC2.2] O grupo de segurança padrão da VPC não deve permitir o tráfego de entrada e saída
- [EC2.3] Os volumes anexados do Amazon EBS devem ser criptografados em repouso.
- As instâncias EC2 interrompidas devem ser removidas após um período de tempo especificado
- [EC2.6] O registro de fluxo de VPC deve ser ativado em todas as VPCs

- As instâncias do EC2 devem usar o Instance Metadata Service Version 2 (IMDSv2)
- As instâncias do Amazon EC2 não devem ter um endereço IPv4 público
- O Amazon EC2 deve ser configurado para usar endpoints da VPC criados para o serviço Amazon EC2
- [EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22
- [EC2.14] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 3389
- As sub-redes do Amazon EC2 não devem atribuir automaticamente endereços IP públicos
- As listas de controle de acesso à rede não utilizadas devem ser removidas
- As instâncias do Amazon EC2 não devem usar vários ENIs
- Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas
- [EC2.20] Ambos os túneis VPN para uma conexão VPN Site-to-Site devem estar ativos AWS
- [PCI.EC2.3] Os grupos de segurança do Amazon EC2 devem ser removidos
- Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- Os modelos de lançamento do Amazon EC2 não devem atribuir IPs públicos às interfaces de rede
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.51] Os endpoints da Client VPN do EC2 devem ter o registro em log de conexão do cliente habilitado
- Os repositórios privados do ECR devem ter a digitalização de imagens configurada
- [ECR.2] Os repositórios privados do ECR devem ter a imutabilidade da tag configurada
- Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário.
- As definições de tarefas do ECS devem ter uma configuração de registro em log
- [EFS.1] O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS
- [EFS.2] Os volumes do Amazon EFS devem estar em planos de backup
- Os pontos de acesso do EFS devem impor um diretório raiz
- Os pontos de acesso do EFS devem impor uma identidade de usuário
- [EFS.5] Os pontos de acesso do EFS devem ser marcados

- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- Os endpoints do cluster EKS não devem ser acessíveis ao público
- Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [ELBv2.1] O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS
- [ELB.2] Os balanceadores de carga clássicos com ouvintes SSL/HTTPS devem usar um certificado fornecido pelo AWS Certificate Manager
- Os receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS
- O Application Load Balancer deve ser configurado para eliminar cabeçalhos http
- [ELB.8] Os balanceadores de carga clássicos com ouvintes SSL devem usar uma política de segurança predefinida que tenha uma duração forte AWS Config
- Os Classic Load Balancers devem ter o balanceador de carga entre zonas habilitado
- O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.16] Os balanceadores de carga de aplicativos devem ser associados a uma ACL da web AWS WAF
- [ElastiCache.1] Os clusters ElastiCache Redis devem ter o backup automático ativado
- [ElastiCache.6] ElastiCache para grupos de replicação do Redis antes da versão 6.0 deve usar o Redis AUTH
- [ElastiCache.7] os ElastiCache clusters não devem usar o grupo de sub-rede padrão
- [ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de integridade aprimorados habilitados
- [ElasticBeanstalk.2] As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas
- [ElasticBeanstalk.3] O Elastic Beanstalk deve transmitir registros para CloudWatch
- [EMR.1] Os nós primários do cluster do Amazon EMR não devem ter endereços IP públicos
- [ES.1] Os domínios do devem ter a criptografia em repouso habilitada.
- [ES.2] Os domínios do Elasticsearch não devem ser publicamente acessíveis
- Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós
- [ES.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado
- [EventBridge.2] ônibus de EventBridge eventos devem ser etiquetados

- [EventBridge.3] os ônibus de eventos EventBridge personalizados devem ter uma política baseada em recursos anexada
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- Os AWS Glue trabalhos [Glue.1] devem ser marcados
- [GuardDuty.1] GuardDuty deve ser ativado
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] Os GuardDuty IPsets devem ser marcados
- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [IAM.1] As políticas do não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do não devem ter políticas do IAM anexadas
- [IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos
- [IAM.4] A chave de acesso do usuário raiz do não deve existir
- [IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console
- As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.18] Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support
- [PCI.IAM.6] A MFA deve estar habilitada para todos os usuários do
- As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.24] As funções do IAM devem ser marcadas
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloudShellFullAccess
- [IoT.1] perfis de AWS IoT Core segurança devem ser marcados
- [IoT.2] as ações de AWS IoT Core mitigação devem ser marcadas

- [IoT.3] as AWS IoT Core dimensões devem ser marcadas
- [IoT.4] os AWS IoT Core autorizadores devem ser marcados
- [IoT.5] aliases de AWS IoT Core função devem ser marcados
- As AWS IoT Core políticas [IoT.6] devem ser marcadas
- Os fluxos do Kinesis devem ser criptografados em repouso
- As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- [Macie.1] O Amazon Macie deve estar ativado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve ser ativada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- [MQ.4] Os corretores do Amazon MQ devem ser marcados
- Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- [MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch
- Os instantâneos do cluster de banco de dados Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- Os clusters de banco de dados Neptune devem ter backups automatizados habilitados
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.7] Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos

- [Neptune.9] Os clusters de banco de dados do Neptune devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.1] Os firewalls do Network Firewall devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.2] O registro do Firewall de Rede deve estar ativado
- [NetworkFirewall.3] As políticas de Firewall de Rede devem ter pelo menos um grupo de regras associado
- [NetworkFirewall.4] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar pacotes completos
- [NetworkFirewall.5] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar para pacotes fragmentados
- [NetworkFirewall.6] O grupo de regras do Stateless Network Firewall não deve estar vazio
- [NetworkFirewall.9] Os firewalls do Firewall de Rede devem ter a proteção contra exclusão ativada
- Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada
- Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público
- Os OpenSearch domínios [Opensearch.3] devem criptografar os dados enviados entre os nós
- O registro de erros de OpenSearch domínio [Opensearch.4] nos CloudWatch registros deve estar ativado
- Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado
- Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados
- Os OpenSearch domínios [Opensearch.7] devem ter um controle de acesso refinado ativado
- [Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente
- Os OpenSearch domínios [Opensearch.9] devem ser marcados
- Os OpenSearch domínios [Opensearch.10] devem ter a atualização de software mais recente instalada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [RDS.1] Os instantâneos do RDS devem ser privados
- [RDS.3] As instâncias de banco de dados do RDS devem ter a criptografia em repouso habilitada.
- As instâncias de banco de dados do RDS devem ser configuradas com várias zonas de disponibilidade
- [RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada

- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados
- [Redshift.12] As assinaturas de notificação de eventos do Redshift devem ser marcadas
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas
- [S3.8] Os buckets de uso geral do S3 devem bloquear o acesso público
- [SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet
- [SageMaker.2] as instâncias do SageMaker notebook devem ser iniciadas em uma VPC personalizada
- [SageMaker.3] Os usuários não devem ter acesso root às instâncias do SageMaker notebook
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [SES.1] As listas de contatos do SES devem ser marcadas
- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [SecretsManager.2] Os segredos do Secrets Manager configurados com rotação automática devem girar com sucesso
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [SNS.1] Os tópicos do SNS devem ser criptografados em repouso usando AWS KMS

- [SNS.3] Os tópicos do SNS devem ser marcados
- As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas SQS devem ser marcadas
- [PCI.SSM.1] As instâncias do Amazon EC2 gerenciadas pelo devem ter um status de conformidade de patch de COMPLIANT (Em conformidade) após a instalação do patch
- PCI.SSM.2 As instâncias de Amazon EC2 gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- [StepFunctions.1] As máquinas de estado do Step Functions devem ter o registro ativado
- Os AWS Transfer Family fluxos de trabalho [Transfer.1] devem ser marcados
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.2] As regras regionais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.3] Os grupos de regras regionais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.4] As ACLs regionais AWS WAF clássicas da web devem ter pelo menos uma regra ou grupo de regras
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras
- [WAF.10] as ACLs AWS WAF da web devem ter pelo menos uma regra ou grupo de regras
- [WAF.11] O registro de ACL AWS WAF da web deve estar ativado

Israel (Tel Aviv)

Os controles a seguir não são compatíveis em Israel (Tel Aviv).

- Os certificados importados e emitidos pelo ACM devem ser renovados após um período de tempo especificado
- Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- As rotas do API de Gateway devem especificar um tipo de autorização

- O registro de acesso deve ser configurado para os estágios V2 do API de Gateway
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado
- [AppSync.4] As APIs AWS AppSync do GraphQL devem ser marcadas
- [AppSync.5] As APIs AWS AppSync do GraphQL não devem ser autenticadas com chaves de API
- [Athena.2] Os catálogos de dados do Athena devem ser marcados
- [Athena.3] Os grupos de trabalho do Athena devem ser marcados
- As instâncias do Amazon EC2 lançadas usando as configurações de execução em grupo do Auto Scaling não devem ter endereços IP públicos
- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.2] os pontos de AWS Backup recuperação devem ser marcados
- [Backup.3] os AWS Backup cofres devem ser marcados
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [Backup.5] os planos de AWS Backup backup devem ser marcados
- [CloudFormation.2] as CloudFormation pilhas devem ser marcadas
- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais

- [CodeBuild.2] as variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado
- [CodeBuild.3] Os registros do CodeBuild S3 devem ser criptografados
- [CodeBuild.4] ambientes de CodeBuild projeto devem ter uma duração de registro AWS Config
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [Detetive.1] Os gráficos do comportamento do detetive devem ser marcados
- As instâncias de replicação do PCI.DMS.1 Database Migration Service não devem ser públicas
- [DMS.2] Os certificados DMS devem ser marcados
- [DMS.3] As assinaturas de eventos do DMS devem ser marcadas
- [DMS.4] As instâncias de replicação do DMS devem ser marcadas
- [DMS.5] Os grupos de sub-redes de replicação do DMS devem ser marcados
- As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- Os endpoints do DMS devem usar SSL
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos
- [DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch
- Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- As tabelas do DynamoDB devem estar presentes em um plano de backup
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito

- [EC2.3] Os volumes anexados do Amazon EBS devem ser criptografados em repouso.
- As instâncias EC2 interrompidas devem ser removidas após um período de tempo especificado
- [EC2.6] O registro de fluxo de VPC deve ser ativado em todas as VPCs
- O Amazon EC2 deve ser configurado para usar endpoints da VPC criados para o serviço Amazon EC2
- [EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22
- [EC2.14] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 3389
- Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas
- [EC2.20] Ambos os túneis VPN para uma conexão VPN Site-to-Site devem estar ativos AWS
- [PCI.EC2.3] Os grupos de segurança do Amazon EC2 devem ser removidos
- Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- Os modelos de lançamento do Amazon EC2 não devem atribuir IPs públicos às interfaces de rede
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.33] Os anexos do gateway de trânsito EC2 devem ser marcados
- [EC2.34] As tabelas de rotas do gateway de trânsito EC2 devem ser marcadas
- [EC2.40] Os gateways NAT EC2 devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.51] Os endpoints da Client VPN do EC2 devem ter o registro em log de conexão do cliente habilitado
- [EC2.52] Os gateways de trânsito do EC2 devem ser marcados
- [ECR.2] Os repositórios privados do ECR devem ter a imutabilidade da tag configurada
- Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário.
- As definições de tarefas do ECS devem ter uma configuração de registro em log
- [EFS.1] O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS
- [EFS.2] Os volumes do Amazon EFS devem estar em planos de backup

- Os pontos de acesso do EFS devem impor um diretório raiz
- Os pontos de acesso do EFS devem impor uma identidade de usuário
- [EFS.5] Os pontos de acesso do EFS devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- Os endpoints do cluster EKS não devem ser acessíveis ao público
- Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [EKS.6] Os clusters EKS devem ser marcados
- [EKS.7] As configurações do provedor de identidade EKS devem ser marcadas
- [EKS.8] Os clusters do EKS devem ter o registro em log de auditoria habilitado
- [ELBv2.1] O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS
- [ELB.2] Os balanceadores de carga clássicos com ouvintes SSL/HTTPS devem usar um certificado fornecido pelo AWS Certificate Manager
- O Application Load Balancer deve ser configurado para eliminar cabeçalhos http
- [ELB.6] Os balanceadores de carga de aplicativos, gateways e redes devem ter a proteção contra exclusão ativada
- [ELB.8] Os balanceadores de carga clássicos com ouvintes SSL devem usar uma política de segurança predefinida que tenha uma duração forte AWS Config
- Balanceadores de carga de aplicações, redes e gateways não abrangem várias zonas de disponibilidade
- O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.16] Os balanceadores de carga de aplicativos devem ser associados a uma ACL da web AWS WAF
- [ElastiCache.1] Os clusters ElastiCache Redis devem ter o backup automático ativado
- [ElastiCache.2] ElastiCache para clusters de cache Redis deve ter a atualização automática de versão secundária habilitada
- [ElastiCache.3] ElastiCache para grupos de replicação do Redis, o failover automático deve estar ativado
- [ElastiCache.4] ElastiCache para Redis, os grupos de replicação devem ser criptografados em repouso

- [ElastiCache.5] ElastiCache para Redis, os grupos de replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache para grupos de replicação do Redis antes da versão 6.0 deve usar o Redis AUTH
- [ElastiCache.7] os ElastiCache clusters não devem usar o grupo de sub-rede padrão
- [ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de integridade aprimorados habilitados
- [ElasticBeanstalk.2] As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas
- [ElasticBeanstalk.3] O Elastic Beanstalk deve transmitir registros para CloudWatch
- [EMR.1] Os nós primários do cluster do Amazon EMR não devem ter endereços IP públicos
- [ES.1] Os domínios do devem ter a criptografia em repouso habilitada.
- [ES.2] Os domínios do Elasticsearch não devem ser publicamente acessíveis
- Os domínios do Elasticsearch devem criptografar os dados enviados entre os nós
- [ES.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado
- [EventBridge.2] ônibus de EventBridge eventos devem ser etiquetados
- [EventBridge.3] os ônibus de eventos EventBridge personalizados devem ter uma política baseada em recursos anexada
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [GuardDuty.1] GuardDuty deve ser ativado
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] Os GuardDuty IPsets devem ser marcados
- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [IAM.1] As políticas do não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do não devem ter políticas do IAM anexadas
- [IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos
- [IAM.4] A chave de acesso do usuário raiz do não deve existir

- [IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- [IAM.7] As políticas de senha para usuários do IAM devem ter configurações fortes
- As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- [IAM.10] As políticas de senha para usuários do IAM devem ter durações fortes AWS Config
- 1.5 Certifique-se de que política de senha do IAM exija pelo menos uma letra maiúscula
- 1.6 Certifique-se de que política de senha do IAM exija pelo menos uma letra minúscula
- 1.7 Certifique-se de que política de senha do IAM exija pelo menos um símbolo
- Certifique-se de que política de senha do IAM exija pelo menos um número
- 1.9 Certifique-se de que a política de senha do IAM exija um comprimento mínimo de 14 ou mais
- 1.10 Certifique-se de que a política de senha do IAM impeça a reutilização de senhas
- 1.11 Certifique-se de que a política de senha do IAM expire senhas em até 90 dias ou menos
- [IAM.18] Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support
- [PCI.IAM.6] A MFA deve estar habilitada para todos os usuários do
- As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.23] Os analisadores do IAM Access Analyzer devem ser marcados
- [IAM.24] As funções do IAM devem ser marcadas
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloudShellFullAccess
- [IAM.28] O analisador de acesso externo do IAM Access Analyzer deve estar ativado
- [IoT.1] perfis de AWS IoT Core segurança devem ser marcados
- [IoT.2] as ações de AWS IoT Core mitigação devem ser marcadas
- [IoT.3] as AWS IoT Core dimensões devem ser marcadas
- [IoT.4] os AWS IoT Core autorizadores devem ser marcados
- [IoT.5] aliases de AWS IoT Core função devem ser marcados
- As AWS IoT Core políticas [IoT.6] devem ser marcadas

- Os fluxos do Kinesis devem ser criptografados em repouso
- [Kinesis.2] Os streams do Kinesis devem ser marcados
- As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- [Macie.1] O Amazon Macie deve estar ativado
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- [MQ.4] Os corretores do Amazon MQ devem ser marcados
- Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- [MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch
- Os instantâneos do cluster de banco de dados Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- Os clusters de banco de dados Neptune devem ter backups automatizados habilitados
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.7] Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- [Neptune.9] Os clusters de banco de dados do Neptune devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.1] Os firewalls do Network Firewall devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.2] O registro do Firewall de Rede deve estar ativado

- [NetworkFirewall.3] As políticas de Firewall de Rede devem ter pelo menos um grupo de regras associado
- [NetworkFirewall.4] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar pacotes completos
- [NetworkFirewall.5] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar para pacotes fragmentados
- [NetworkFirewall.6] O grupo de regras do Stateless Network Firewall não deve estar vazio
- [NetworkFirewall.9] Os firewalls do Firewall de Rede devem ter a proteção contra exclusão ativada
- Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada
- Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público
- Os OpenSearch domínios [Opensearch.3] devem criptografar os dados enviados entre os nós
- O registro de erros de OpenSearch domínio [Opensearch.4] nos CloudWatch registros deve estar ativado
- Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado
- Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados
- Os OpenSearch domínios [Opensearch.7] devem ter um controle de acesso refinado ativado
- [Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente
- Os OpenSearch domínios [Opensearch.9] devem ser marcados
- Os OpenSearch domínios [Opensearch.10] devem ter a atualização de software mais recente instalada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [PCA.1] a autoridade de certificação AWS Private CA raiz deve ser desativada
- [RDS.1] Os instantâneos do RDS devem ser privados
- Os instantâneos do cluster do RDS e os instantâneos do banco de dados devem ser criptografados em repouso
- [RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada
- [RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada
- A autenticação do IAM deve ser configurada para instâncias do RDS
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.15] Os clusters de banco de dados do RDS devem ser configurados para várias zonas de disponibilidade

- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [RDS.28] Os clusters de banco de dados do RDS devem ser marcados
- [RDS.29] Os instantâneos do cluster de banco de dados do RDS devem ser marcados
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [RDS.34] Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch
- Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- Os clusters do Amazon Redshift devem ter instantâneos automáticos habilitados
- Os clusters do Amazon Redshift não devem usar o nome de usuário Admin padrão
- [Redshift.9] Os clusters do Redshift não devem usar o nome do banco de dados padrão
- [Redshift.12] As assinaturas de notificação de eventos do Redshift devem ser marcadas
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas
- [S3.2] Os buckets de uso geral do S3 devem bloquear o acesso público de leitura
- [S3.3] Os buckets de uso geral do S3 devem bloquear o acesso público de gravação
- [S3.8] Os buckets de uso geral do S3 devem bloquear o acesso público
- [S3.9] Os buckets de uso geral do S3 devem ter o registro de acesso ao servidor ativado
- [SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet
- [SageMaker.2] as instâncias do SageMaker notebook devem ser iniciadas em uma VPC personalizada
- [SageMaker.3] Os usuários não devem ter acesso root às instâncias do SageMaker notebook

- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [SES.1] As listas de contatos do SES devem ser marcadas
- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [SecretsManager.1] Os segredos do Secrets Manager devem ter a rotação automática ativada
- [SecretsManager.2] Os segredos do Secrets Manager configurados com rotação automática devem girar com sucesso
- [SecretsManager.3] Remover segredos não utilizados do Secrets Manager
- [SecretsManager.4] Os segredos do Secrets Manager devem ser alternados dentro de um determinado número de dias
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [SNS.1] Os tópicos do SNS devem ser criptografados em repouso usando AWS KMS
- [SNS.3] Os tópicos do SNS devem ser marcados
- As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas SQS devem ser marcadas
- [SSM.1] As instâncias do Amazon EC2 devem ser gerenciadas por AWS Systems Manager
- [PCI.SSM.1] As instâncias do Amazon EC2 gerenciadas pelo devem ter um status de conformidade de patch de COMPLIANT (Em conformidade) após a instalação do patch
- PCI.SSM.2 As instâncias de Amazon EC2 gerenciadas pelo Systems Manager devem ter um status de conformidade de associação de COMPATÍVEL
- Os documentos SSM não devem ser públicos
- [StepFunctions.1] As máquinas de estado do Step Functions devem ter o registro ativado
- [StepFunctions.2] As atividades do Step Functions devem ser marcadas
- Os AWS Transfer Family fluxos de trabalho [Transfer.1] devem ser marcados
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.2] As regras regionais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.3] Os grupos de regras regionais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.4] As ACLs regionais AWS WAF clássicas da web devem ter pelo menos uma regra ou grupo de regras

- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras
- [WAF.11] O registro de ACL AWS WAF da web deve estar ativado
- As AWS WAF regras [WAF.12] devem ter métricas habilitadas CloudWatch

Oriente Médio (Barém)

Os controles a seguir não são compatíveis no Oriente Médio (Bahrein).

- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do Amazon DocumentDB devem ser criptografados em repouso

- Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos
- [DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch
- Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- [EC2.20] Ambos os túneis VPN para uma conexão VPN Site-to-Site devem estar ativos AWS
- Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de integridade aprimorados habilitados
- [ElasticBeanstalk.3] O Elastic Beanstalk deve transmitir registros para CloudWatch
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [GuardDuty.1] GuardDuty deve ser ativado
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada
- A autenticação do IAM deve ser configurada para instâncias do RDS

- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.15] Os clusters de banco de dados do RDS devem ser configurados para várias zonas de disponibilidade
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- O Amazon Redshift deve ter as atualizações automáticas para as versões principais habilitadas
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [PCI.SSM.1] As instâncias do Amazon EC2 gerenciadas pelo devem ter um status de conformidade de patch de COMPLIANT (Em conformidade) após a instalação do patch
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

Oriente Médio (Emirados Árabes Unidos)

Os controles a seguir não são compatíveis no Oriente Médio (UAE).

- Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits

- [ApiGateway.1] O REST do API Gateway WebSocket e o registro de execução da API devem estar habilitados
- As rotas do API de Gateway devem especificar um tipo de autorização
- O registro de acesso deve ser configurado para os estágios V2 do API de Gateway
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado
- [AppSync.5] As APIs AWS AppSync do GraphQL não devem ser autenticadas com chaves de API
- [Athena.2] Os catálogos de dados do Athena devem ser marcados
- [Athena.3] Os grupos de trabalho do Athena devem ser marcados
- [AutoScaling.1] Grupos de Auto Scaling associados a um balanceador de carga devem usar verificações de integridade do ELB
- [Backup.1] os pontos de AWS Backup recuperação devem ser criptografados em repouso
- [Backup.2] os pontos de AWS Backup recuperação devem ser marcados
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [Backup.5] os planos de AWS Backup backup devem ser marcados
- [CloudFormation.2] as CloudFormation pilhas devem ser marcadas
- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CloudTrail.1] CloudTrail deve ser habilitado e configurado com pelo menos uma trilha multirregional que inclua eventos de gerenciamento de leitura e gravação

- [CloudTrail.6] Certifique-se de que o bucket do S3 usado para armazenar CloudTrail registros não esteja acessível ao público
- [CloudWatch.15] CloudWatch os alarmes devem ter ações especificadas configuradas
- [CloudWatch.16] os grupos de CloudWatch registros devem ser mantidos por um período de tempo especificado
- [CloudWatch.17] ações de CloudWatch alarme devem ser ativadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais
- [CodeBuild.2] as variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado
- [CodeBuild.3] Os registros do CodeBuild S3 devem ser criptografados
- [CodeBuild.4] ambientes de CodeBuild projeto devem ter uma duração de registro AWS Config
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [Detetive.1] Os gráficos do comportamento do detetive devem ser marcados
- As instâncias de replicação do PCI.DMS.1 Database Migration Service não devem ser públicas
- [DMS.2] Os certificados DMS devem ser marcados
- [DMS.3] As assinaturas de eventos do DMS devem ser marcadas
- [DMS.4] As instâncias de replicação do DMS devem ser marcadas
- [DMS.5] Os grupos de sub-redes de replicação do DMS devem ser marcados
- As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- Os endpoints do DMS devem usar SSL
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do Amazon DocumentDB devem ser criptografados em repouso

- Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos
- [DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch
- Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- As tabelas do DynamoDB devem estar presentes em um plano de backup
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- [EC2.3] Os volumes anexados do Amazon EBS devem ser criptografados em repouso.
- As instâncias EC2 interrompidas devem ser removidas após um período de tempo especificado
- [EC2.6] O registro de fluxo de VPC deve ser ativado em todas as VPCs
- As instâncias do EC2 devem usar o Instance Metadata Service Version 2 (IMDSv2)
- [PCI.EC2.4] Os EIPs do EC2 não utilizados devem ser removidos
- [EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22
- [EC2.14] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 3389
- [PCI.EC2.3] Os grupos de segurança do Amazon EC2 devem ser removidos
- Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- Os modelos de lançamento do Amazon EC2 não devem atribuir IPs públicos às interfaces de rede
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.51] Os endpoints da Client VPN do EC2 devem ter o registro em log de conexão do cliente habilitado
- Os repositórios privados do ECR devem ter a digitalização de imagens configurada
- [ECR.2] Os repositórios privados do ECR devem ter a imutabilidade da tag configurada
- Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário.
- As definições de tarefas do ECS devem ter uma configuração de registro em log
- [EFS.1] O Elastic File System deve ser configurado para criptografar dados de arquivos em repouso usando AWS KMS

- [EFS.2] Os volumes do Amazon EFS devem estar em planos de backup
- Os pontos de acesso do EFS devem impor um diretório raiz
- Os pontos de acesso do EFS devem impor uma identidade de usuário
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- Os endpoints do cluster EKS não devem ser acessíveis ao público
- Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [ELBv2.1] O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS
- Os receptores do Classic Load Balancer devem ser configurados com terminação HTTPS ou TLS
- Os Classic Load Balancers devem ter o balanceador de carga entre zonas habilitado
- O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.16] Os balanceadores de carga de aplicativos devem ser associados a uma ACL da web AWS WAF
- [ElastiCache.1] Os clusters ElastiCache Redis devem ter o backup automático ativado
- [ElastiCache.2] ElastiCache para clusters de cache Redis deve ter a atualização automática de versão secundária habilitada
- [ElastiCache.3] ElastiCache para grupos de replicação do Redis, o failover automático deve estar ativado
- [ElastiCache.4] ElastiCache para Redis, os grupos de replicação devem ser criptografados em repouso
- [ElastiCache.5] ElastiCache para Redis, os grupos de replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache para grupos de replicação do Redis antes da versão 6.0 deve usar o Redis AUTH
- [ElastiCache.7] os ElastiCache clusters não devem usar o grupo de sub-rede padrão
- [ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de integridade aprimorados habilitados
- [ElasticBeanstalk.2] As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas
- [ElasticBeanstalk.3] O Elastic Beanstalk deve transmitir registros para CloudWatch

- [EMR.1] Os nós primários do cluster do Amazon EMR não devem ter endereços IP públicos
- [EventBridge.2] ônibus de EventBridge eventos devem ser etiquetados
- [EventBridge.3] os ônibus de eventos EventBridge personalizados devem ter uma política baseada em recursos anexada
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [GuardDuty.1] GuardDuty deve ser ativado
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] Os GuardDuty IPsets devem ser marcados
- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [IAM.1] As políticas do não devem permitir privilégios administrativos completos "*"
- [IAM.2] Os usuários do não devem ter políticas do IAM anexadas
- [IAM.3] As chaves de acesso dos usuários do IAM devem ser mudadas a cada 90 dias ou menos
- [IAM.4] A chave de acesso do usuário raiz do não deve existir
- [IAM.5] A MFA deve estar habilitada para todos os usuários do IAM com uma senha do console
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- [IAM.18] Certifique-se de que uma função de suporte tenha sido criada para gerenciar incidentes com AWS Support
- [PCI.IAM.6] A MFA deve estar habilitada para todos os usuários do
- As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- As credenciais de usuário do IAM não utilizadas devem ser removidas
- [IAM.24] As funções do IAM devem ser marcadas
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos

- [IAM.27] As identidades do IAM não devem ter a política anexada AWSCloudShellFullAccess
- [IoT.1] perfis de AWS IoT Core segurança devem ser marcados
- [IoT.2] as ações de AWS IoT Core mitigação devem ser marcadas
- [IoT.3] as AWS IoT Core dimensões devem ser marcadas
- Os fluxos do Kinesis devem ser criptografados em repouso
- As políticas gerenciadas pelo cliente do IAM não devem permitir ações de descriptografia em todas as chaves do KMS
- As entidades principais do IAM não devem ter políticas incorporadas do IAM que permitam ações de descriptografia em todas as chaves do KMS
- A rotação de AWS KMS teclas [KMS.4] deve estar ativada
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- [Macie.1] O Amazon Macie deve estar ativado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve ser ativada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- [MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch
- Os instantâneos do cluster de banco de dados Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- Os clusters de banco de dados Neptune devem ter backups automatizados habilitados
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.7] Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- [Neptune.9] Os clusters de banco de dados do Neptune devem ser implantados em várias zonas de disponibilidade

- [NetworkFirewall.1] Os firewalls do Network Firewall devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.2] O registro do Firewall de Rede deve estar ativado
- [NetworkFirewall.3] As políticas de Firewall de Rede devem ter pelo menos um grupo de regras associado
- [NetworkFirewall.4] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar pacotes completos
- [NetworkFirewall.5] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar para pacotes fragmentados
- [NetworkFirewall.6] O grupo de regras do Stateless Network Firewall não deve estar vazio
- [NetworkFirewall.7] Os firewalls do Firewall de Rede devem ser marcados
- [NetworkFirewall.8] As políticas de firewall do Network Firewall devem ser marcadas
- [NetworkFirewall.9] Os firewalls do Firewall de Rede devem ter a proteção contra exclusão ativada
- Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada
- Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público
- Os OpenSearch domínios [Opensearch.3] devem criptografar os dados enviados entre os nós
- O registro de erros de OpenSearch domínio [Opensearch.4] nos CloudWatch registros deve estar ativado
- Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado
- Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados
- Os OpenSearch domínios [Opensearch.7] devem ter um controle de acesso refinado ativado
- [Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente
- Os OpenSearch domínios [Opensearch.9] devem ser marcados
- Os OpenSearch domínios [Opensearch.10] devem ter a atualização de software mais recente instalada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [RDS.1] Os instantâneos do RDS devem ser privados
- [RDS.2] As instâncias de banco de dados do RDS devem proibir o acesso público, conforme determinado pela duração PubliclyAccessible AWS Config
- [RDS.3] As instâncias de banco de dados do RDS devem ter a criptografia em repouso habilitada.

- As instâncias de banco de dados do RDS devem ser configuradas com várias zonas de disponibilidade
- O monitoramento aprimorado deve ser configurado para instâncias de banco de dados do RDS
- [RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada
- As instâncias do RDS devem ter backups automáticos habilitados
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- [Redshift.9] Os clusters do Redshift não devem usar o nome do banco de dados padrão
- [Redshift.12] As assinaturas de notificação de eventos do Redshift devem ser marcadas
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.2] Os buckets de uso geral do S3 devem bloquear o acesso público de leitura
- [S3.3] Os buckets de uso geral do S3 devem bloquear o acesso público de gravação
- [S3.5] Os buckets de uso geral do S3 devem exigir solicitações de uso de SSL
- [S3.6] As políticas de bucket de uso geral do S3 devem restringir o acesso a outros Contas da AWS
- [S3.14] Os buckets de uso geral do S3 devem ter o controle de versão ativado
- [SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet
- [SageMaker.2] as instâncias do SageMaker notebook devem ser iniciadas em uma VPC personalizada
- [SageMaker.3] Os usuários não devem ter acesso root às instâncias do SageMaker notebook

- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [SES.1] As listas de contatos do SES devem ser marcadas
- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [SecretsManager.1] Os segredos do Secrets Manager devem ter a rotação automática ativada
- [SecretsManager.2] Os segredos do Secrets Manager configurados com rotação automática devem girar com sucesso
- [SecretsManager.3] Remover segredos não utilizados do Secrets Manager
- [SecretsManager.4] Os segredos do Secrets Manager devem ser alternados dentro de um determinado número de dias
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [SNS.1] Os tópicos do SNS devem ser criptografados em repouso usando AWS KMS
- [SNS.3] Os tópicos do SNS devem ser marcados
- As filas do Amazon SQS devem ser criptografadas em repouso
- [SQS.2] As filas SQS devem ser marcadas
- [SSM.1] As instâncias do Amazon EC2 devem ser gerenciadas por AWS Systems Manager
- [StepFunctions.1] As máquinas de estado do Step Functions devem ter o registro ativado
- Os AWS Transfer Family fluxos de trabalho [Transfer.1] devem ser marcados
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.2] As regras regionais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.3] Os grupos de regras regionais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.4] As ACLs regionais AWS WAF clássicas da web devem ter pelo menos uma regra ou grupo de regras
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras
- [WAF.10] as ACLs AWS WAF da web devem ter pelo menos uma regra ou grupo de regras

- [WAF.11] O registro de ACL AWS WAF da web deve estar ativado

América do Sul (São Paulo)

Os controles a seguir não são compatíveis na América do Sul (São Paulo).

- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.

- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [IoT.1] perfis de AWS IoT Core segurança devem ser marcados
- [IoT.2] as ações de AWS IoT Core mitigação devem ser marcadas
- [IoT.3] as AWS IoT Core dimensões devem ser marcadas
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada
- A autenticação do IAM deve ser configurada para instâncias do RDS
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.15] Os clusters de banco de dados do RDS devem ser configurados para várias zonas de disponibilidade
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição

- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras

AWS GovCloud (Leste dos EUA)

Os controles a seguir não são suportados em AWS GovCloud (Leste dos EUA).

- Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- [ACM.3] Os certificados ACM devem ser marcados
- [Conta.1] As informações de contato de segurança devem ser fornecidas para um Conta da AWS
- [A conta.2] Contas da AWS deve fazer parte de uma organização AWS Organizations
- Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end
- Os estágios da API REST de Gateway devem ter o rastreamento AWS X-Ray habilitado.
- O API Gateway deve ser associado a uma WAF Web ACL
- As rotas do API de Gateway devem especificar um tipo de autorização
- O registro de acesso deve ser configurado para os estágios V2 do API de Gateway
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado
- [AppSync.4] As APIs AWS AppSync do GraphQL devem ser marcadas
- [AppSync.5] As APIs AWS AppSync do GraphQL não devem ser autenticadas com chaves de API
- [Athena.2] Os catálogos de dados do Athena devem ser marcados
- [Athena.3] Os grupos de trabalho do Athena devem ser marcados
- [AutoScaling.2] O grupo Amazon EC2 Auto Scaling deve abranger várias zonas de disponibilidade
- [AutoScaling.3] As configurações de lançamento de grupos do Auto Scaling devem configurar as instâncias do EC2 para exigir o Instance Metadata Service Version 2 (IMDSv2)
- [AutoScaling.6] Os grupos de Auto Scaling devem usar vários tipos de instância em várias zonas de disponibilidade
- [AutoScaling.9] Os grupos do Amazon EC2 Auto Scaling devem usar os modelos de lançamento do Amazon EC2
- [AutoScaling.10] Os grupos do EC2 Auto Scaling devem ser marcados

- As instâncias do Amazon EC2 lançadas usando as configurações de execução em grupo do Auto Scaling não devem ter endereços IP públicos
- [Backup.2] os pontos de AWS Backup recuperação devem ser marcados
- [Backup.3] os AWS Backup cofres devem ser marcados
- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [Backup.5] os planos de AWS Backup backup devem ser marcados
- [CloudFormation.2] as CloudFormation pilhas devem ser marcadas
- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CloudTrail.9] CloudTrail trilhas devem ser marcadas
- [CloudWatch.15] CloudWatch os alarmes devem ter ações especificadas configuradas
- [CloudWatch.16] os grupos de CloudWatch registros devem ser mantidos por um período de tempo especificado
- [CloudWatch.17] ações de CloudWatch alarme devem ser ativadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais
- [CodeBuild.2] as variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado

- [CodeBuild.3] Os registros do CodeBuild S3 devem ser criptografados
- [CodeBuild.4] ambientes de CodeBuild projeto devem ter uma duração de registro AWS Config
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [Detetive.1] Os gráficos do comportamento do detetive devem ser marcados
- [DMS.2] Os certificados DMS devem ser marcados
- [DMS.3] As assinaturas de eventos do DMS devem ser marcadas
- [DMS.4] As instâncias de replicação do DMS devem ser marcadas
- [DMS.5] Os grupos de sub-redes de replicação do DMS devem ser marcados
- As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- Os endpoints do DMS devem usar SSL
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos
- [DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch
- Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- As tabelas do DynamoDB devem escalar automaticamente a capacidade de acordo com a demanda
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- As tabelas do DynamoDB devem estar presentes em um plano de backup
- [DynamoDB.5] As tabelas do DynamoDB devem ser marcadas
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito

- As sub-redes do Amazon EC2 não devem atribuir automaticamente endereços IP públicos
- As listas de controle de acesso à rede não utilizadas devem ser removidas
- As instâncias do Amazon EC2 não devem usar vários ENIs
- As ACLs de rede não devem permitir a entrada de 0.0.0.0/0 para a porta 22 ou porta 3389
- [PCI.EC2.3] Os grupos de segurança do Amazon EC2 devem ser removidos
- Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- Os modelos de lançamento do Amazon EC2 não devem atribuir IPs públicos às interfaces de rede
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.33] Os anexos do gateway de trânsito EC2 devem ser marcados
- [EC2.34] As tabelas de rotas do gateway de trânsito EC2 devem ser marcadas
- [EC2.35] As interfaces de rede EC2 devem ser marcadas
- [EC2.36] Os gateways de clientes do EC2 devem ser marcados
- [EC2.37] Os endereços IP elásticos do EC2 devem ser marcados
- [EC2.38] As instâncias do EC2 devem ser marcadas
- [EC2.39] Os gateways de internet EC2 devem ser marcados
- [EC2.40] Os gateways NAT EC2 devem ser marcados
- [EC2.41] As ACLs de rede EC2 devem ser marcadas
- [EC2.42] As tabelas de rotas do EC2 devem ser marcadas
- [EC2.43] Grupos de segurança do EC2 devem ser marcados
- [EC2.44] As sub-redes do EC2 devem ser marcadas
- [EC2.45] Os volumes do EC2 devem ser marcados
- [EC2.46] Amazon VPCs devem ser marcadas
- [EC2.47] Os serviços de endpoint da Amazon VPC devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.49] As conexões de emparelhamento da Amazon VPC devem ser marcadas
- [EC2.50] Os gateways de VPN EC2 devem ser marcados
- [EC2.52] Os gateways de trânsito do EC2 devem ser marcados
- Os repositórios privados do ECR devem ter a digitalização de imagens configurada
- [ECR.2] Os repositórios privados do ECR devem ter a imutabilidade da tag configurada

- Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário.
- As definições de tarefas do ECS não devem compartilhar o namespace do processo do host
- Os contêineres ECS devem ser executados sem privilégios
- Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz
- Os segredos não devem ser passados como variáveis de ambiente do contêiner
- As definições de tarefas do ECS devem ter uma configuração de registro em log
- Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate
- Os clusters do ECS devem usar Container Insights
- [ECS.13] Os serviços do ECS devem ser marcados
- [ECS.14] Os clusters ECS devem ser marcados
- [ECS.15] As definições de tarefas do ECS devem ser marcadas
- [EFS.2] Os volumes do Amazon EFS devem estar em planos de backup
- Os pontos de acesso do EFS devem impor um diretório raiz
- Os pontos de acesso do EFS devem impor uma identidade de usuário
- [EFS.5] Os pontos de acesso do EFS devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- Os endpoints do cluster EKS não devem ser acessíveis ao público
- Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [EKS.6] Os clusters EKS devem ser marcados
- [EKS.7] As configurações do provedor de identidade EKS devem ser marcadas
- [EKS.8] Os clusters do EKS devem ter o registro em log de auditoria habilitado
- [ELB.2] Os balanceadores de carga clássicos com ouvintes SSL/HTTPS devem usar um certificado fornecido pelo AWS Certificate Manager
- [ELB.8] Os balanceadores de carga clássicos com ouvintes SSL devem usar uma política de segurança predefinida que tenha uma duração forte AWS Config
- Verifica se o Classic Load Balancer abrange várias zonas de disponibilidade (AZs).

- O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- Balanceadores de carga de aplicações, redes e gateways não abrangem várias zonas de disponibilidade
- O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.16] Os balanceadores de carga de aplicativos devem ser associados a uma ACL da web AWS WAF
- [ElastiCache.1] Os clusters ElastiCache Redis devem ter o backup automático ativado
- [ElastiCache.2] ElastiCache para clusters de cache Redis deve ter a atualização automática de versão secundária habilitada
- [ElastiCache.3] ElastiCache para grupos de replicação do Redis, o failover automático deve estar ativado
- [ElastiCache.4] ElastiCache para Redis, os grupos de replicação devem ser criptografados em repouso
- [ElastiCache.5] ElastiCache para Redis, os grupos de replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache para grupos de replicação do Redis antes da versão 6.0 deve usar o Redis AUTH
- [ElastiCache.7] os ElastiCache clusters não devem usar o grupo de sub-rede padrão
- [ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de integridade aprimorados habilitados
- [ElasticBeanstalk.2] As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas
- [ElasticBeanstalk.3] O Elastic Beanstalk deve transmitir registros para CloudWatch
- [EMR.2] A configuração de bloqueio de acesso público do Amazon EMR deve estar habilitada
- [ES.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado
- [ES.9] Os domínios do Elasticsearch devem ser marcados
- [EventBridge.2] ônibus de EventBridge eventos devem ser etiquetados
- [EventBridge.3] os ônibus de eventos EventBridge personalizados devem ter uma política baseada em recursos anexada
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada

- [FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- Os AWS Glue trabalhos [Glue.1] devem ser marcados
- [GuardDuty.1] GuardDuty deve ser ativado
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] Os GuardDuty IPsets devem ser marcados
- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.23] Os analisadores do IAM Access Analyzer devem ser marcados
- [IAM.24] As funções do IAM devem ser marcadas
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos
- [IAM.28] O analisador de acesso externo do IAM Access Analyzer deve estar ativado
- [IoT.1] perfis de AWS IoT Core segurança devem ser marcados
- [IoT.2] as ações de AWS IoT Core mitigação devem ser marcadas
- [IoT.3] as AWS IoT Core dimensões devem ser marcadas
- [IoT.4] os AWS IoT Core autorizadores devem ser marcados
- [IoT.5] aliases de AWS IoT Core função devem ser marcados
- As AWS IoT Core políticas [IoT.6] devem ser marcadas
- Os fluxos do Kinesis devem ser criptografados em repouso
- [Kinesis.2] Os streams do Kinesis devem ser marcados
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- [Lambda.6] As funções Lambda devem ser marcadas
- [Macie.1] O Amazon Macie deve estar ativado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve ser ativada

- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- [MQ.4] Os corretores do Amazon MQ devem ser marcados
- Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- [MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch
- Os instantâneos do cluster de banco de dados Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- Os clusters de banco de dados Neptune devem ter backups automatizados habilitados
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.7] Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- [Neptune.9] Os clusters de banco de dados do Neptune devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.1] Os firewalls do Network Firewall devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.2] O registro do Firewall de Rede deve estar ativado
- [NetworkFirewall.3] As políticas de Firewall de Rede devem ter pelo menos um grupo de regras associado
- [NetworkFirewall.4] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar pacotes completos
- [NetworkFirewall.5] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar para pacotes fragmentados
- [NetworkFirewall.6] O grupo de regras do Stateless Network Firewall não deve estar vazio
- [NetworkFirewall.7] Os firewalls do Firewall de Rede devem ser marcados

- [NetworkFirewall.8] As políticas de firewall do Network Firewall devem ser marcadas
- [NetworkFirewall.9] Os firewalls do Firewall de Rede devem ter a proteção contra exclusão ativada
- Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada
- Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público
- Os OpenSearch domínios [Opensearch.3] devem criptografar os dados enviados entre os nós
- O registro de erros de OpenSearch domínio [Opensearch.4] nos CloudWatch registros deve estar ativado
- Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado
- Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados
- Os OpenSearch domínios [Opensearch.7] devem ter um controle de acesso refinado ativado
- [Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente
- Os OpenSearch domínios [Opensearch.9] devem ser marcados
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [PCA.1] a autoridade de certificação AWS Private CA raiz deve ser desativada
- A autenticação do IAM deve ser configurada para instâncias do RDS
- [RDS.13] As atualizações automáticas de versões secundárias do RDS devem ser ativadas
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.15] Os clusters de banco de dados do RDS devem ser configurados para várias zonas de disponibilidade
- Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [RDS.28] Os clusters de banco de dados do RDS devem ser marcados
- [RDS.29] Os instantâneos do cluster de banco de dados do RDS devem ser marcados
- [RDS.30] As instâncias de banco de dados do RDS devem ser marcadas
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [RDS.32] Os instantâneos do banco de dados do RDS devem ser marcados

- [RDS.33] Os grupos de sub-redes do banco de dados do RDS devem ser marcados
- [RDS.34] Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch
- Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- Os clusters do Redshift devem usar roteamento de VPC aprimorado
- Os clusters do Amazon Redshift não devem usar o nome de usuário Admin padrão
- [Redshift.9] Os clusters do Redshift não devem usar o nome do banco de dados padrão
- [Redshift.10] Os clusters do Redshift devem ser criptografados em repouso
- [Redshift.11] Os clusters do Redshift devem ser marcados
- [Redshift.12] As assinaturas de notificação de eventos do Redshift devem ser marcadas
- [Redshift.13] Os instantâneos do cluster do Redshift devem ser marcados
- [Redshift.14] Os grupos de sub-redes do cluster Redshift devem ser marcados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas
- [S3.8] Os buckets de uso geral do S3 devem bloquear o acesso público
- [S3.10] Os buckets de uso geral do S3 com controle de versão ativado devem ter configurações de ciclo de vida
- [S3.11] Os buckets de uso geral do S3 devem ter as notificações de eventos ativadas
- [S3.12] As ACLs não devem ser usadas para gerenciar o acesso do usuário aos buckets de uso geral do S3
- [S3.13] Os buckets de uso geral do S3 devem ter configurações de ciclo de vida
- [S3.14] Os buckets de uso geral do S3 devem ter o controle de versão ativado
- [S3.20] Os buckets de uso geral do S3 devem ter a exclusão de MFA habilitada
- [SageMaker.1] As instâncias de SageMaker notebooks da Amazon não devem ter acesso direto à Internet
- [SageMaker.2] as instâncias do SageMaker notebook devem ser iniciadas em uma VPC personalizada

- [SageMaker.3] Os usuários não devem ter acesso root às instâncias do SageMaker notebook
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [SES.1] As listas de contatos do SES devem ser marcadas
- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [SecretsManager.3] Remover segredos não utilizados do Secrets Manager
- [SecretsManager.4] Os segredos do Secrets Manager devem ser alternados dentro de um determinado número de dias
- [SecretsManager.5] Os segredos do Secrets Manager devem ser marcados
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS
- [SNS.3] Os tópicos do SNS devem ser marcados
- [SQS.2] As filas SQS devem ser marcadas
- Os documentos SSM não devem ser públicos
- [StepFunctions.1] As máquinas de estado do Step Functions devem ter o registro ativado
- [StepFunctions.2] As atividades do Step Functions devem ser marcadas
- Os AWS Transfer Family fluxos de trabalho [Transfer.1] devem ser marcados
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.2] As regras regionais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.3] Os grupos de regras regionais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.4] As ACLs regionais AWS WAF clássicas da web devem ter pelo menos uma regra ou grupo de regras
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras
- [WAF.10] as ACLs AWS WAF da web devem ter pelo menos uma regra ou grupo de regras
- [WAF.11] O registro de ACL AWS WAF da web deve estar ativado
- As AWS WAF regras [WAF.12] devem ter métricas habilitadas CloudWatch

AWS GovCloud (Oeste dos EUA)

Os controles a seguir não são suportados em AWS GovCloud (Oeste dos EUA).

- Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits
- [ACM.3] Os certificados ACM devem ser marcados
- [Conta.1] As informações de contato de segurança devem ser fornecidas para um Conta da AWS
- [A conta.2] Contas da AWS deve fazer parte de uma organização AWS Organizations
- Os estágios da API REST de Gateway devem ser configurados para usar certificados SSL para autenticação de back-end
- Os estágios da API REST de Gateway devem ter o rastreamento AWS X-Ray habilitado.
- O API Gateway deve ser associado a uma WAF Web ACL
- As rotas do API de Gateway devem especificar um tipo de autorização
- O registro de acesso deve ser configurado para os estágios V2 do API de Gateway
- [AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado
- [AppSync.4] As APIs AWS AppSync do GraphQL devem ser marcadas
- [AppSync.5] As APIs AWS AppSync do GraphQL não devem ser autenticadas com chaves de API
- [Athena.2] Os catálogos de dados do Athena devem ser marcados
- [Athena.3] Os grupos de trabalho do Athena devem ser marcados
- [AutoScaling.2] O grupo Amazon EC2 Auto Scaling deve abranger várias zonas de disponibilidade
- [AutoScaling.3] As configurações de lançamento de grupos do Auto Scaling devem configurar as instâncias do EC2 para exigir o Instance Metadata Service Version 2 (IMDSv2)
- [AutoScaling.6] Os grupos de Auto Scaling devem usar vários tipos de instância em várias zonas de disponibilidade
- [AutoScaling.9] Os grupos do Amazon EC2 Auto Scaling devem usar os modelos de lançamento do Amazon EC2
- [AutoScaling.10] Os grupos do EC2 Auto Scaling devem ser marcados
- As instâncias do Amazon EC2 lançadas usando as configurações de execução em grupo do Auto Scaling não devem ter endereços IP públicos
- [Backup.2] os pontos de AWS Backup recuperação devem ser marcados
- [Backup.3] os AWS Backup cofres devem ser marcados

- [Backup.4] os planos de AWS Backup relatórios devem ser marcados
- [Backup.5] os planos de AWS Backup backup devem ser marcados
- [CloudFormation.2] as CloudFormation pilhas devem ser marcadas
- [CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado
- [CloudFront.3] CloudFront as distribuições devem exigir criptografia em trânsito
- [CloudFront.4] CloudFront as distribuições devem ter o failover de origem configurado
- [CloudFront.5] CloudFront as distribuições devem ter o registro ativado
- [CloudFront.6] as CloudFront distribuições devem ter o WAF ativado
- [CloudFront.7] CloudFront as distribuições devem usar certificados SSL/TLS personalizados
- [CloudFront.8] CloudFront as distribuições devem usar o SNI para atender às solicitações HTTPS
- [CloudFront.9] CloudFront as distribuições devem criptografar o tráfego para origens personalizadas
- [CloudFront.10] CloudFront as distribuições não devem usar protocolos SSL obsoletos entre pontos de presença e origens personalizadas
- [CloudFront.12] CloudFront as distribuições não devem apontar para origens inexistentes do S3
- [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem
- [CloudFront.14] as CloudFront distribuições devem ser marcadas
- [CloudTrail.9] CloudTrail trilhas devem ser marcadas
- [CloudWatch.15] CloudWatch os alarmes devem ter ações especificadas configuradas
- [CloudWatch.16] os grupos de CloudWatch registros devem ser mantidos por um período de tempo especificado
- [CloudWatch.17] ações de CloudWatch alarme devem ser ativadas
- [CodeArtifact.1] CodeArtifact repositórios devem ser marcados
- [CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais
- [CodeBuild.2] as variáveis de ambiente CodeBuild do projeto não devem conter credenciais de texto não criptografado
- [CodeBuild.3] Os registros do CodeBuild S3 devem ser criptografados
- [CodeBuild.4] ambientes de CodeBuild projeto devem ter uma duração de registro AWS Config
- [DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso
- [Detetive.1] Os gráficos do comportamento do detetive devem ser marcados

- [DMS.2] Os certificados DMS devem ser marcados
- [DMS.3] As assinaturas de eventos do DMS devem ser marcadas
- [DMS.4] As instâncias de replicação do DMS devem ser marcadas
- [DMS.5] Os grupos de sub-redes de replicação do DMS devem ser marcados
- As instâncias de replicação do DMS devem ter a atualização automática de versões secundárias habilitada
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado
- Os endpoints do DMS devem usar SSL
- [DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada
- [DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado
- [DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado
- Os clusters do Amazon DocumentDB devem ser criptografados em repouso
- Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado
- Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos
- [DocumentDB.4] Os clusters do Amazon DocumentDB devem publicar registros de auditoria no Logs CloudWatch
- Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada
- As tabelas do DynamoDB devem escalar automaticamente a capacidade de acordo com a demanda
- Os clusters do DynamoDB Accelerator (DAX) devem ser criptografados em repouso
- As tabelas do DynamoDB devem estar presentes em um plano de backup
- [DynamoDB.5] As tabelas do DynamoDB devem ser marcadas
- [DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito
- As sub-redes do Amazon EC2 não devem atribuir automaticamente endereços IP públicos
- As listas de controle de acesso à rede não utilizadas devem ser removidas
- As instâncias do Amazon EC2 não devem usar vários ENIs
- As ACLs de rede não devem permitir a entrada de 0.0.0.0/0 para a porta 22 ou porta 3389

- [PCI.EC2.3] Os grupos de segurança do Amazon EC2 devem ser removidos
- Os EC2 Transit Gateways não devem aceitar automaticamente solicitações de anexos de VPC
- Os tipos de instância paravirtual do Amazon EC2 não devem ser usados
- Os modelos de lançamento do Amazon EC2 não devem atribuir IPs públicos às interfaces de rede
- [EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup
- [EC2.33] Os anexos do gateway de trânsito EC2 devem ser marcados
- [EC2.34] As tabelas de rotas do gateway de trânsito EC2 devem ser marcadas
- [EC2.35] As interfaces de rede EC2 devem ser marcadas
- [EC2.36] Os gateways de clientes do EC2 devem ser marcados
- [EC2.37] Os endereços IP elásticos do EC2 devem ser marcados
- [EC2.38] As instâncias do EC2 devem ser marcadas
- [EC2.39] Os gateways de internet EC2 devem ser marcados
- [EC2.40] Os gateways NAT EC2 devem ser marcados
- [EC2.41] As ACLs de rede EC2 devem ser marcadas
- [EC2.42] As tabelas de rotas do EC2 devem ser marcadas
- [EC2.43] Grupos de segurança do EC2 devem ser marcados
- [EC2.44] As sub-redes do EC2 devem ser marcadas
- [EC2.45] Os volumes do EC2 devem ser marcados
- [EC2.46] Amazon VPCs devem ser marcadas
- [EC2.47] Os serviços de endpoint da Amazon VPC devem ser marcados
- [EC2.48] Os registros de fluxo da Amazon VPC devem ser marcados
- [EC2.49] As conexões de emparelhamento da Amazon VPC devem ser marcadas
- [EC2.50] Os gateways de VPN EC2 devem ser marcados
- [EC2.52] Os gateways de trânsito do EC2 devem ser marcados
- Os repositórios privados do ECR devem ter a digitalização de imagens configurada
- [ECR.2] Os repositórios privados do ECR devem ter a imutabilidade da tag configurada
- Os repositórios ECR devem ter pelo menos uma política de ciclo de vida configurada
- [ECR.4] Os repositórios públicos do ECR devem ser marcados
- As definições de tarefas do Amazon ECS devem ter modos de rede seguros e definições de usuário.

- As definições de tarefas do ECS não devem compartilhar o namespace do processo do host
- Os contêineres ECS devem ser executados sem privilégios
- Os contêineres do ECS devem ser limitados ao acesso somente leitura aos sistemas de arquivos raiz
- Os segredos não devem ser passados como variáveis de ambiente do contêiner
- As definições de tarefas do ECS devem ter uma configuração de registro em log
- Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate
- Os clusters do ECS devem usar Container Insights
- [ECS.13] Os serviços do ECS devem ser marcados
- [ECS.14] Os clusters ECS devem ser marcados
- [ECS.15] As definições de tarefas do ECS devem ser marcadas
- [EFS.2] Os volumes do Amazon EFS devem estar em planos de backup
- Os pontos de acesso do EFS devem impor um diretório raiz
- Os pontos de acesso do EFS devem impor uma identidade de usuário
- [EFS.5] Os pontos de acesso do EFS devem ser marcados
- [EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública
- Os endpoints do cluster EKS não devem ser acessíveis ao público
- Os clusters EKS devem ser executados em uma versão compatível do Kubernetes
- [EKS.3] Os clusters EKS devem usar segredos criptografados do Kubernetes
- [EKS.6] Os clusters EKS devem ser marcados
- [EKS.7] As configurações do provedor de identidade EKS devem ser marcadas
- [EKS.8] Os clusters do EKS devem ter o registro em log de auditoria habilitado
- Verifica se o Classic Load Balancer abrange várias zonas de disponibilidade (AZs).
- O Application Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- Balanceadores de carga de aplicações, redes e gateways não abrangem várias zonas de disponibilidade
- O Classic Load Balancer deve ser configurado com o modo defensivo ou com o modo de mitigação de dessincronização mais rigoroso
- [ELB.16] Os balanceadores de carga de aplicativos devem ser associados a uma ACL da web AWS WAF

- [ElastiCache.1] Os clusters ElastiCache Redis devem ter o backup automático ativado
- [ElastiCache.2] ElastiCache para clusters de cache Redis deve ter a atualização automática de versão secundária habilitada
- [ElastiCache.3] ElastiCache para grupos de replicação do Redis, o failover automático deve estar ativado
- [ElastiCache.4] ElastiCache para Redis, os grupos de replicação devem ser criptografados em repouso
- [ElastiCache.5] ElastiCache para Redis, os grupos de replicação devem ser criptografados em trânsito
- [ElastiCache.6] ElastiCache para grupos de replicação do Redis antes da versão 6.0 deve usar o Redis AUTH
- [ElastiCache.7] os ElastiCache clusters não devem usar o grupo de sub-rede padrão
- [ElasticBeanstalk.1] Os ambientes do Elastic Beanstalk devem ter os relatórios de integridade aprimorados habilitados
- [ElasticBeanstalk.2] As atualizações da plataforma gerenciada do Elastic Beanstalk devem estar habilitadas
- [ElasticBeanstalk.3] O Elastic Beanstalk deve transmitir registros para CloudWatch
- [EMR.2] A configuração de bloqueio de acesso público do Amazon EMR deve estar habilitada
- [ES.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado
- [ES.9] Os domínios do Elasticsearch devem ser marcados
- [EventBridge.2] ônibus de EventBridge eventos devem ser etiquetados
- [EventBridge.3] os ônibus de eventos EventBridge personalizados devem ter uma política baseada em recursos anexada
- [EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada
- [FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configurados para copiar tags para backups e volumes.
- [FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups
- [GlobalAccelerator.1] Os aceleradores do Global Accelerator devem ser marcados
- Os AWS Glue trabalhos [Glue.1] devem ser marcados
- [GuardDuty.2] GuardDuty os filtros devem ser marcados
- [GuardDuty.3] Os GuardDuty IPsets devem ser marcados

- [GuardDuty.4] os GuardDuty detectores devem ser marcados
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- [IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz
- As políticas gerenciadas pelo cliente do IAM que você cria não devem permitir ações curingas para serviços.
- [IAM.23] Os analisadores do IAM Access Analyzer devem ser marcados
- [IAM.24] As funções do IAM devem ser marcadas
- [IAM.25] Os usuários do IAM devem ser marcados
- [IAM.28] O analisador de acesso externo do IAM Access Analyzer deve estar ativado
- [IoT.1] perfis de AWS IoT Core segurança devem ser marcados
- [IoT.2] as ações de AWS IoT Core mitigação devem ser marcadas
- [IoT.3] as AWS IoT Core dimensões devem ser marcadas
- [IoT.4] os AWS IoT Core autorizadores devem ser marcados
- [IoT.5] aliases de AWS IoT Core função devem ser marcados
- As AWS IoT Core políticas [IoT.6] devem ser marcadas
- Os fluxos do Kinesis devem ser criptografados em repouso
- [Kinesis.2] Os streams do Kinesis devem ser marcados
- [Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade
- [Lambda.6] As funções Lambda devem ser marcadas
- [Macie.1] O Amazon Macie deve estar ativado
- [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve ser ativada
- [MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch
- [MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada
- [MQ.4] Os corretores do Amazon MQ devem ser marcados
- Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera
- Os agentes do RabbitMQ devem usar o modo de implantação de cluster
- Os clusters MSK devem ser criptografados em trânsito entre os nós do agente
- [MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado
- Os clusters de banco de dados Neptune devem ser criptografados em repouso

- [Neptune.2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch
- Os instantâneos do cluster de banco de dados Neptune não devem ser públicos
- [Neptune.4] Os clusters de banco de dados Neptune devem ter a proteção contra exclusão ativada
- Os clusters de banco de dados Neptune devem ter backups automatizados habilitados
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [Neptune.7] Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada
- Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos
- [Neptune.9] Os clusters de banco de dados do Neptune devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.1] Os firewalls do Network Firewall devem ser implantados em várias zonas de disponibilidade
- [NetworkFirewall.2] O registro do Firewall de Rede deve estar ativado
- [NetworkFirewall.3] As políticas de Firewall de Rede devem ter pelo menos um grupo de regras associado
- [NetworkFirewall.4] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar pacotes completos
- [NetworkFirewall.5] A ação sem estado padrão para políticas de Firewall de Rede deve ser descartar ou encaminhar para pacotes fragmentados
- [NetworkFirewall.6] O grupo de regras do Stateless Network Firewall não deve estar vazio
- [NetworkFirewall.7] Os firewalls do Firewall de Rede devem ser marcados
- [NetworkFirewall.8] As políticas de firewall do Network Firewall devem ser marcadas
- [NetworkFirewall.9] Os firewalls do Firewall de Rede devem ter a proteção contra exclusão ativada
- Os OpenSearch domínios [Opensearch.1] devem ter a criptografia em repouso ativada
- Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público
- Os OpenSearch domínios [Opensearch.3] devem criptografar os dados enviados entre os nós
- O registro de erros de OpenSearch domínio [Opensearch.4] nos CloudWatch registros deve estar ativado
- Os OpenSearch domínios [Opensearch.5] devem ter o registro de auditoria ativado
- Os OpenSearch domínios [Opensearch.6] devem ter pelo menos três nós de dados

- Os OpenSearch domínios [Opensearch.7] devem ter um controle de acesso refinado ativado
- [Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente
- Os OpenSearch domínios [Opensearch.9] devem ser marcados
- Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados
- [PCA.1] a autoridade de certificação AWS Private CA raiz deve ser desativada
- A autenticação do IAM deve ser configurada para instâncias do RDS
- [RDS.13] As atualizações automáticas de versões secundárias do RDS devem ser ativadas
- [RDS.14] Os clusters do Amazon Aurora devem ter o backtracking ativado
- [RDS.15] Os clusters de banco de dados do RDS devem ser configurados para várias zonas de disponibilidade
- Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- Os clusters de banco de dados do RDS devem usar um nome de usuário de administrador personalizado
- As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup
- Os clusters de banco de dados Neptune devem ser criptografados em repouso
- [RDS.28] Os clusters de banco de dados do RDS devem ser marcados
- [RDS.29] Os instantâneos do cluster de banco de dados do RDS devem ser marcados
- [RDS.30] As instâncias de banco de dados do RDS devem ser marcadas
- [RDS.31] Os grupos de segurança do RDS DB devem ser marcados
- [RDS.32] Os instantâneos do banco de dados do RDS devem ser marcados
- [RDS.33] Os grupos de sub-redes do banco de dados do RDS devem ser marcados
- [RDS.34] Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch
- Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada
- Os clusters do Redshift devem usar roteamento de VPC aprimorado
- Os clusters do Amazon Redshift não devem usar o nome de usuário Admin padrão
- [Redshift.9] Os clusters do Redshift não devem usar o nome do banco de dados padrão
- [Redshift.10] Os clusters do Redshift devem ser criptografados em repouso

- [Redshift.11] Os clusters do Redshift devem ser marcados
- [Redshift.12] As assinaturas de notificação de eventos do Redshift devem ser marcadas
- [Redshift.13] Os instantâneos do cluster do Redshift devem ser marcados
- [Redshift.14] Os grupos de sub-redes do cluster Redshift devem ser marcados
- [Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas
- [Route53.1] As verificações de saúde do Route 53 devem ser marcadas
- As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS
- [S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas
- [S3.8] Os buckets de uso geral do S3 devem bloquear o acesso público
- [S3.10] Os buckets de uso geral do S3 com controle de versão ativado devem ter configurações de ciclo de vida
- [S3.11] Os buckets de uso geral do S3 devem ter as notificações de eventos ativadas
- [S3.12] As ACLs não devem ser usadas para gerenciar o acesso do usuário aos buckets de uso geral do S3
- [S3.13] Os buckets de uso geral do S3 devem ter configurações de ciclo de vida
- [S3.14] Os buckets de uso geral do S3 devem ter o controle de versão ativado
- [S3.20] Os buckets de uso geral do S3 devem ter a exclusão de MFA habilitada
- [SageMaker.2] as instâncias do SageMaker notebook devem ser iniciadas em uma VPC personalizada
- [SageMaker.3] Os usuários não devem ter acesso root às instâncias do SageMaker notebook
- [SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1
- [SES.1] As listas de contatos do SES devem ser marcadas
- [SES.2] Os conjuntos de configuração do SES devem ser marcados
- [SecretsManager.3] Remover segredos não utilizados do Secrets Manager
- [SecretsManager.4] Os segredos do Secrets Manager devem ser alternados dentro de um determinado número de dias
- [SecretsManager.5] Os segredos do Secrets Manager devem ser marcados
- [ServiceCatalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS

- [SNS.3] Os tópicos do SNS devem ser marcados
- [SQS.2] As filas SQS devem ser marcadas
- Os documentos SSM não devem ser públicos
- [StepFunctions.1] As máquinas de estado do Step Functions devem ter o registro ativado
- [StepFunctions.2] As atividades do Step Functions devem ser marcadas
- Os AWS Transfer Family fluxos de trabalho [Transfer.1] devem ser marcados
- [Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints
- [WAF.1] O registro AWS WAF clássico do Global Web ACL deve estar ativado
- [WAF.2] As regras regionais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.3] Os grupos de regras regionais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.4] As ACLs regionais AWS WAF clássicas da web devem ter pelo menos uma regra ou grupo de regras
- [WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição
- [WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra
- [WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras
- [WAF.10] as ACLs AWS WAF da web devem ter pelo menos uma regra ou grupo de regras
- [WAF.11] O registro de ACL AWS WAF da web deve estar ativado
- As AWS WAF regras [WAF.12] devem ter métricas habilitadas CloudWatch

Desabilitar o Security Hub

> **Note**
>
> Se você usar a configuração central, o administrador delegado do AWS Security Hub poderá criar políticas de configuração que desabilitem o Security Hub em contas e unidades organizacionais (OUs) específicas e o mantenham habilitado em outras. As políticas de configuração entram em vigor na sua região inicial e em todas as regiões vinculadas. Para obter mais informações, consulte Como a configuração central funciona.

Para desabilitar o Security Hub, é possível usar o console do Security Hub, a API do Security Hub ou a AWS CLI.

Quando o Security Hub é desabilitado para uma conta, ocorre o seguinte:

- Nenhuma descoberta nova será processada para a conta.
- Depois de 90 dias, suas descobertas, insights existentes e quaisquer definições de configuração do Security Hub serão excluídos e não poderão ser recuperados.

  Se você quiser salvar suas descobertas existentes, precisará exportá-las antes de desabilitar o Security Hub. Para obter mais informações, consulte the section called “Efeito das ações da conta nos dados do Security Hub”.
- Todos os padrões habilitados serão desabilitados.

Você não pode desabilitar o Security Hub nos casos a seguir:

- Sua conta é uma conta de administrador do Security Hub designado para sua organização. Se você usar a configuração central, não poderá associar uma política de configuração que desabilite o Security Hub à conta do administrador delegado. A associação pode ser ter êxito para outras contas, mas o Security Hub não aplica essa política à conta do administrador delegado.
- Sua conta é uma conta de administrador do Security Hub por convite, e você tem contas de membros que estão habilitadas. Antes de poder desabilitar o Security Hub, você deve desassociar todas as contas de membro. Consulte the section called “Desassociar contas-membro”.

Antes de desabilitar o Security Hub para uma conta-membro, a conta deve ser desassociada da sua conta de administrador. Para uma conta da organização, somente a conta do administrador pode desassociar as contas dos membros. Para obter mais informações, consulte the section called "Desassociação de contas-membro da organização". Para contas convidadas manualmente, a conta do administrador ou a conta de membro podem desassociar a conta de membro. Para obter mais informações, consulte the section called "Desassociar contas-membro" ou the section called "Desassociando-se da sua conta de administrador". A desassociação não será necessária se você usar a configuração central, porque é possível criar uma política que desabilite o Security Hub em contas-membro específicas.

Quando você desabilita o Security Hub em uma conta, ele é desabilitado somente na região atual. Entretanto, se você usar a configuração central para desabilitar o Security Hub em contas específicas, ele será desabilitado na região inicial e em todas as regiões vinculadas.

Escolha seu método preferido e siga as etapas para desabilitar o Security Hub.

Security Hub console

Para desabilitar o Security Hub

1. Abra o console do AWS Security Hub em https://console.aws.amazon.com/securityhub/.
2. No painel de navegação, escolha Configurações.
3. Na página Configurações, selecione Geral.
4. Em Desabilitar o AWS Security Hub, escolha Desabilitar o AWS Security Hub. Em seguida, escolha Desabilitar o AWS Security Hub novamente.

Security Hub API

Para desabilitar o Security Hub

Invoque a API `DisableSecurityHub`.

AWS CLI

Para desabilitar o Security Hub

Execute o comando `disable-security-hub`.

Exemplo de comando:

```
aws securityhub disable-security-hub
```

Log de alterações dos controles do Security Hub

O registro de alterações a seguir rastreia alterações materiais nos controles de AWS Security Hub segurança existentes, o que pode resultar em alterações no status geral de um controle e no status de conformidade de suas descobertas. Para obter informações sobre como o Security Hub avalia o status do controle, consulte Status de conformidade e status de controle. As alterações podem levar alguns dias após sua entrada nesse registro para afetar tudo Regiões da AWS em que o controle está disponível.

Esse log rastreia as mudanças ocorridas desde abril de 2023.

Selecione um controle para ver mais detalhes sobre ele. As alterações de título são anotadas na descrição detalhada de cada controle por 90 dias.

Data da mudança	Título e ID do controle	Descrição de alteração
8 de maio de 2024	[S3.20] Os buckets de uso geral do S3 devem ter a exclusão de MFA habilitada	Esse controle verifica se um bucket versionado de uso geral do Amazon S3 tem a exclusão de autenticação multifator (MFA) ativada. Anteriormente, o controle produzia uma `FAILED` descoberta para buckets que têm uma configuração de ciclo de vida. No entanto, a exclusão de MFA com controle de versão não pode ser habilitada em um bucket que tenha uma configuração de ciclo de vida. O Security

Data da mudança	Título e ID do controle	Descrição de alteração
		Hub atualizou o controle para não produzir descobertas para buckets que têm uma configuração de ciclo de vida. A descrição do controle foi atualizada para refletir o comportamento atual.
2 de maio de 2024	Os clusters EKS devem ser executados em uma versão compatível do Kubernetes	O Security Hub atualizou a versão mais antiga compatível do Kubernetes na qual o cluster Amazon EKS pode ser executado para produzir uma descoberta aprovada. A versão atual mais antiga compatível é o Kubernetes `1.26`.

Data da mudança	Título e ID do controle	Descrição de alteração
30 de abril de 2024	[CloudTrail.3] Pelo menos uma CloudTrail trilha deve ser ativada	O título de controle alterado de CloudTrail deve ser ativado para Pelo menos uma CloudTrail trilha deve ser ativada. Atualmente, esse controle produz uma `PASSED` descoberta se um Conta da AWS tiver pelo menos uma CloudTrail trilha ativada. O título e a descrição foram alterados para refletir com precisão o comportamento atual.

Data da mudança	Título e ID do controle	Descrição de alteração
29 de abril de 2024	[AutoScaling.1] Grupos de Auto Scaling associados a um balanceador de carga devem usar verificações de integridade do ELB	O título de controle alterado de grupos de Auto Scaling associados a um Classic Load Balancer deve usar verificaç ões de integridade do balanceador de carga para grupos de Auto Scaling associado s a um balancead or de carga devem usar verificações de integridade do ELB. Atualmente, esse controle avalia os balanceadores de carga de aplicativos, gateways, redes e clássicos. O título e a descrição foram alterados para refletir com precisão o comportamento atual.

Data da mudança	Título e ID do controle	Descrição de alteração
19 de abril de 2024	[CloudTrail.1] CloudTrail deve ser habilitado e configurado com pelo menos uma trilha multirregional que inclua eventos de gerenciamento de leitura e gravação	O controle verifica se AWS CloudTrail está habilitado e configurado com pelo menos uma trilha multirregional que inclui eventos de gerenciamento de leitura e gravação. Anteriormente, o controle gerava `PASSED` descobertas incorretamente quando uma conta era CloudTrail ativada e configurada com pelo menos uma trilha multirregional, mesmo que nenhuma trilha capturasse eventos de gerenciamento de leitura e gravação. O controle agora gera uma `PASSED` descoberta somente quando CloudTrail está habilitado e configurado com pelo menos uma trilha multirregional que captura eventos de gerenciamento de leitura e gravação.

Data da mudança	Título e ID do controle	Descrição de alteração
10 de abril de 2024	[Athena.1] Os grupos de trabalho do Athena devem ser criptografados em repouso	O Security Hub descontinuou esse controle e o removeu de todos os padrões. Os grupos de trabalho do Athena enviam registros para os buckets do Amazon Simple Storage Service (Amazon S3). O Amazon S3 agora fornece criptografia padrão com chaves gerenciadas pelo S3 (SS3-S3) em buckets do S3 novos e existentes.
10 de abril de 2024	[AutoScaling.4] A configuração de inicialização do grupo Auto Scaling não deve ter um limite de salto de resposta de metadados maior que 1	O Security Hub descontinuou esse controle e o removeu de todos os padrões. Os limites de salto de resposta de metadados para instâncias do Amazon Elastic Compute Cloud (Amazon EC2) dependem da carga de trabalho.

Data da mudança	Título e ID do controle	Descrição de alteração
10 de abril de 2024	[CloudFormation.1] CloudFormation as pilhas devem ser integradas ao Simple Notification Service (SNS)	O Security Hub descontinuou esse controle e o removeu de todos os padrões. Integrar AWS CloudFormation pilhas com tópicos do Amazon SNS não é mais uma prática recomendada de segurança. Embora a integração de CloudFormation pilhas importantes com tópicos do SNS possa ser útil, ela não é necessária para todas as pilhas.
10 de abril de 2024	[CodeBuild.5] ambientes de CodeBuild projeto não devem ter o modo privilegiado ativado	O Security Hub descontinuou esse controle e o removeu de todos os padrões. Ativar o modo privilegiado em um CodeBuild projeto não impõe um risco adicional ao ambiente do cliente.

Data da mudança	Título e ID do controle	Descrição de alteração
10 de abril de 2024	[IAM.20] Evite o uso do usuário root	O Security Hub descontinuou esse controle e o removeu de todos os padrões. O objetivo desse controle é coberto por outro controle, [CloudWatch.1] Um filtro métrico de log e um alarme devem existir para uso do usuário “root”.
10 de abril de 2024	[SNS.2] O registro do status de entrega deve ser ativado para mensagens de notificação enviadas para um tópico	O Security Hub descontinuou esse controle e o removeu de todos os padrões. Registrar o status de entrega dos tópicos do SNS não é mais uma prática recomendada de segurança. Embora o registro do status de entrega de tópicos importantes do SNS possa ser útil, ele não é obrigatório para todos os tópicos.

Data da mudança	Título e ID do controle	Descrição de alteração
10 de abril de 2024	[S3.10] Os buckets de uso geral do S3 com controle de versão ativado devem ter configurações de ciclo de vida	O Security Hub removeu esse controle do AWS Foundational Security Best Practices and Service-Managed Standard:. AWS Control Tower O objetivo desse controle é coberto por dois outros controles : [S3.13] Os buckets de uso geral do S3 devem ter configurações de ciclo de vida [S3.14] Os buckets de uso geral do S3 devem ter o controle de versão ativado e. Esse controle ainda faz parte do NIST SP 800-53 Rev. 5.

Data da mudança	Título e ID do controle	Descrição de alteração
10 de abril de 2024	[S3.11] Os buckets de uso geral do S3 devem ter as notificações de eventos ativadas	O Security Hub removeu esse controle do AWS Foundational Security Best Practices and Service-Managed Standard:. AWS Control Tower Embora haja alguns casos em que as notificações de eventos para buckets do S3 sejam úteis, essa não é uma prática recomendada de segurança universal. Esse controle ainda faz parte do NIST SP 800-53 Rev. 5.

Data da mudança	Título e ID do controle	Descrição de alteração
10 de abril de 2024	[SNS.1] Os tópicos do SNS devem ser criptografados em repouso usando AWS KMS	O Security Hub removeu esse controle do AWS Foundational Security Best Practices and Service-Managed Standard:. AWS Control Tower Como o SNS já criptografa tópicos por padrão, usar AWS KMS para criptogra far tópicos não é mais recomendado como uma prática recomendada de segurança. Esse controle ainda faz parte do NIST SP 800-53 Rev. 5.

Data da mudança	Título e ID do controle	Descrição de alteração
8 de abril de 2024	[ELB.6] Os balanceadores de carga de aplicativos, gateways e redes devem ter a proteção contra exclusão ativada	O título de controle alterado de Proteção de exclusão do Application Load Balancer deve estar habilitado para Application, Gateway e Network Load Balancers deve ter a proteção de exclusão ativada. Atualmente, esse controle avalia balanceadores de carga de aplicativos, gateways e redes. O título e a descrição foram alterados para refletir com precisão o comportamento atual.

Data da mudança	Título e ID do controle	Descrição de alteração
22 de março de 2024	[Opensearch.8] As conexões com OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente	O título de controle alterado de Conexões a OpenSearch domínios deve ser criptografado usando TLS 1.2 para Conexões a OpenSearch domínios devem ser criptografadas usando a política de segurança TLS mais recente. Anteriormente, o controle só verificava se as conexões com OpenSearch domínios usavam o TLS 1.2. O controle agora produz uma `PASSED` descoberta se os OpenSearch domínios estão criptografados usando a política de segurança TLS mais recente. O título e a descrição do controle foram atualizados para refletir o comportamento atual.

Data da mudança	Título e ID do controle	Descrição de alteração
22 de março de 2024	[ES.8] As conexões com os domínios do Elasticsearch devem ser criptografadas usando a política de segurança TLS mais recente	O título de controle alterado de Conexões para domínios Elasticsearch deve ser criptografado usando TLS 1.2 para Conexões para domínios Elasticsearch deve ser criptografado usando a política de segurança TLS mais recente. Anteriorm ente, o controle só verificava se as conexões com os domínios do Elasticse arch usavam TLS 1.2. O controle agora produz uma PASSED descoberta se os domínios do Elasticse arch estão criptogra fados usando a política de segurança TLS mais recente. O título e a descrição do controle foram atualizados para refletir o comportam ento atual.

Data da mudança	Título e ID do controle	Descrição de alteração
12 de março de 2024	[S3.1] Os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas	O título alterado da configuração Bloquear acesso público do S3 deve ser ativado para os buckets de uso geral do S3 devem ter as configurações de bloqueio de acesso público ativadas. O Security Hub alterou o título para contabilizar um novo tipo de bucket do S3.
12 de março de 2024	[S3.2] Os buckets de uso geral do S3 devem bloquear o acesso público de leitura	O título alterado dos buckets do S3 deve proibir o acesso público de leitura. Os buckets de uso geral do S3 devem bloquear o acesso público de leitura. O Security Hub alterou o título para contabilizar um novo tipo de bucket do S3.

Data da mudança	Título e ID do controle	Descrição de alteração
12 de março de 2024	[S3.3] Os buckets de uso geral do S3 devem bloquear o acesso público de gravação	O título alterado dos buckets do S3 deve proibir o acesso público de gravação aos buckets de uso geral do S3. Os buckets de uso geral do S3 devem bloquear o acesso público de gravação. O Security Hub alterou o título para contabilizar um novo tipo de bucket do S3.
12 de março de 2024	[S3.5] Os buckets de uso geral do S3 devem exigir solicitações de uso de SSL	O título alterado de buckets do S3 deve exigir solicitações de uso do Secure Socket Layer para buckets de uso geral do S3 devem exigir solicitações de uso de SSL. O Security Hub alterou o título para contabilizar um novo tipo de bucket do S3.

Data da mudança	Título e ID do controle	Descrição de alteração
12 de março de 2024	[S3.6] As políticas de bucket de uso geral do S3 devem restringir o acesso a outros Contas da AWS	O título alterado das permissões do S3 concedidas a outras políticas Contas da AWS no bucket deve ser restrito às políticas de bucket de uso geral do S3. As políticas de bucket devem restringir o acesso a outras. Contas da AWS O Security Hub alterou o título para contabilizar um novo tipo de bucket do S3.
12 de março de 2024	[S3.7] Os buckets de uso geral do S3 devem usar a replicação entre regiões	O título alterado dos buckets do S3 deve ter a replicação entre regiões ativada para os buckets de uso geral do S3 devem usar a replicação entre regiões. O Security Hub alterou o título para contabilizar um novo tipo de bucket do S3.

Data da mudança	Título e ID do controle	Descrição de alteração
12 de março de 2024	[S3.7] Os buckets de uso geral do S3 devem usar a replicação entre regiões	O título alterado dos buckets do S3 deve ter a replicação entre regiões ativada para os buckets de uso geral do S3 devem usar a replicação entre regiões. O Security Hub alterou o título para contabilizar um novo tipo de bucket do S3.
12 de março de 2024	[S3.8] Os buckets de uso geral do S3 devem bloquear o acesso público	O título alterado da configuração S3 Block Public Access deve ser ativado no nível do bucket para buckets de uso geral do S3 devem bloquear o acesso público. O Security Hub alterou o título para contabilizar um novo tipo de bucket do S3.

Data da mudança	Título e ID do controle	Descrição de alteração
12 de março de 2024	[S3.9] Os buckets de uso geral do S3 devem ter o registro de acesso ao servidor ativado	O título alterado do registro de acesso ao servidor do bucket do S3 deve ser ativado para o registro de acesso ao servidor deve ser ativado para buckets de uso geral do S3. O Security Hub alterou o título para contabilizar um novo tipo de bucket do S3.
12 de março de 2024	[S3.10] Os buckets de uso geral do S3 com controle de versão ativado devem ter configurações de ciclo de vida	O título alterado de buckets do S3 com versionamento ativado deve ter políticas de ciclo de vida configuradas para buckets de uso geral do S3 com versionamento ativado devem ter configurações de ciclo de vida. O Security Hub alterou o título para contabilizar um novo tipo de bucket do S3.

Data da mudança	Título e ID do controle	Descrição de alteração
12 de março de 2024	[S3.11] Os buckets de uso geral do S3 devem ter as notificações de eventos ativadas	O título alterado de buckets do S3 deve ter as notificações de eventos ativadas para os buckets de uso geral do S3 devem ter as notificações de eventos ativadas. O Security Hub alterou o título para contabilizar um novo tipo de bucket do S3.
12 de março de 2024	[S3.12] As ACLs não devem ser usadas para gerenciar o acesso do usuário aos buckets de uso geral do S3	O título alterado das listas de controle de acesso (ACLs) do S3 não deve ser usado para gerenciar o acesso do usuário aos buckets para ACLs não deve ser usado para gerenciar o acesso do usuário aos buckets de uso geral do S3. O Security Hub alterou o título para contabilizar um novo tipo de bucket do S3.

Data da mudança	Título e ID do controle	Descrição de alteração
12 de março de 2024	[S3.13] Os buckets de uso geral do S3 devem ter configurações de ciclo de vida	O título alterado de buckets do S3 deve ter políticas de ciclo de vida configuradas para que os buckets de uso geral do S3 tenham configurações de ciclo de vida. O Security Hub alterou o título para contabilizar um novo tipo de bucket do S3.
12 de março de 2024	[S3.14] Os buckets de uso geral do S3 devem ter o controle de versão ativado	O título alterado de buckets do S3 deve usar o controle de versão para buckets de uso geral do S3 deve ter o versionamento ativado. O Security Hub alterou o título para contabilizar um novo tipo de bucket do S3.

Data da mudança	Título e ID do controle	Descrição de alteração
12 de março de 2024	[S3.15] Os buckets de uso geral do S3 devem ter o Object Lock ativado	O título alterado dos buckets do S3 deve ser configurado para usar o Object Lock para os buckets de uso geral do S3 devem ter o Object Lock ativado. O Security Hub alterou o título para contabilizar um novo tipo de bucket do S3.
12 de março de 2024	[S3.17] Os buckets de uso geral do S3 devem ser criptografados em repouso com AWS KMS keys	O título alterado de buckets do S3 deve ser criptografado em repouso AWS KMS keys para buckets de uso geral do S3 deve ser criptografado em repouso com. AWS KMS keys O Security Hub alterou o título para contabilizar um novo tipo de bucket do S3.

Data da mudança	Título e ID do controle	Descrição de alteração
7 de março de 2024	[Lambda.2] As funções do devem usar os tempos de execução mais recentes	O Lambda.2 verifica se as configurações da AWS Lambda função para tempos de execução correspondem aos valores esperados definidos para os tempos de execução suportados em cada idioma. O Security Hub agora suporta `nodejs20.x` e `ruby3.3` como parâmetro.
22 de fevereiro de 2024	[Lambda.2] As funções do devem usar os tempos de execução mais recentes	O Lambda.2 verifica se as configurações da AWS Lambda função para tempos de execução correspondem aos valores esperados definidos para os tempos de execução suportados em cada idioma. O Security Hub agora oferece suporte `dotnet8` como parâmetro.

Data da mudança	Título e ID do controle	Descrição de alteração
5 de fevereiro de 2024	Os clusters EKS devem ser executados em uma versão compatível do Kubernetes	O Security Hub atualizou a versão mais antiga compatível do Kubernetes na qual o cluster Amazon EKS pode ser executado para produzir uma descoberta aprovada. A versão atual mais antiga compatível é o Kubernetes `1.25`.

Data da mudança	Título e ID do controle	Descrição de alteração
10 de janeiro de 2024	[CodeBuild.1] Os URLs do repositório CodeBuild de origem do Bitbucket não devem conter credenciais confidenciais	Os URLs alterados do título CodeBuild GitHub ou do repositório de origem do Bitbucket devem usar OAuth para que os URLs do repositório CodeBuild de origem do Bitbucket não contenham credenciais confidenciais. O Security Hub removeu a menção ao OAuth porque outros métodos de conexão também podem ser seguros. O Security Hub removeu a menção GitHub porque não é mais possível ter um token de acesso pessoal ou nome de usuário e senha nos URLs do repositório de GitHub origem.

Data da mudança	Título e ID do controle	Descrição de alteração
8 de janeiro de 2024	[Lambda.2] As funções do devem usar os tempos de execução mais recentes	O Lambda.2 verifica se as configurações da AWS Lambda função para tempos de execução correspondem aos valores esperados definidos para os tempos de execução suportados em cada idioma. O Security Hub não oferece mais suporte a `go1.x` e `java8` como parâmetros porque esses são runtimes descontinuados.

Data da mudança	Título e ID do controle	Descrição de alteração
29 de dezembro de 2023	[RDS.7] Os clusters RDS devem ter a proteção contra exclusão ativada	O RDS.8 verifica se uma instância de banco de dados Amazon RDS que use um dos mecanismos de banco de dados com suporte tem a proteção contra exclusão habilitada. O Security Hub agora oferece suporte a `custom-oracle-ee`, `oracle-ee-cdb` e `oracle-se2-cdb` como mecanismos de banco de dados.

Data da mudança	Título e ID do controle	Descrição de alteração
22 de dezembro de 2023	[Lambda.2] As funções do devem usar os tempos de execução mais recentes	O Lambda.2 verifica se as configurações da AWS Lambda função para tempos de execução correspondem aos valores esperados definidos para os tempos de execução suportados em cada idioma. O Security Hub agora oferece suporte a `java21` e `python3.12` como parâmetros. O Security Hub não é mais compatível com `ruby2.7` como parâmetro.

Data da mudança	Título e ID do controle	Descrição de alteração
15 de dezembro de 2023	[CloudFront.1] CloudFront as distribuições devem ter um objeto raiz padrão configurado	CloudFront.1 verifica se uma CloudFront distribuição da Amazon tem um objeto raiz padrão configurado. O Security Hub reduziu a severidade desse controle de CRÍTICA para ALTA, porque adicionar o objeto raiz padrão é uma recomendação que depende da aplicação do usuário e dos requisitos específicos.
5 de dezembro de 2023	[EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22	Título de controle alterado de Grupos de segurança não deve permitir a entrada de 0.0.0.0/0 na porta 22 para Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22.

Data da mudança	Título e ID do controle	Descrição de alteração
5 de dezembro de 2023	[EC2.14] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 3389	Título de controle alterado de Certifique-se de que nenhum grupo de segurança permita a entrada de 0.0.0.0/0 na porta 3389 para Grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 3389.

Data da mudança	Título e ID do controle	Descrição de alteração
5 de dezembro de 2023	[RDS.9] As instâncias de banco de dados do RDS devem publicar registros no Logs CloudWatch	O título de controle alterado do Registro do banco de dados deve ser habilitado para que as instâncias de banco de dados do RDS publiquem os registros nos CloudWatch registros. O Security Hub identificou que esse controle só verifica se os registros estão publicados no Amazon CloudWatch Logs e não verifica se os registros do RDS estão habilitados. O controle produz uma PASSED descoberta se as instâncias de banco de dados do RDS estão configuradas para publicar registros no CloudWatch Logs. O título de controle foi atualizado para refletir o comportamento atual.

Data da mudança	Título e ID do controle	Descrição de alteração
17 de novembro de 2023	Grupos de segurança não devem permitir acesso irrestrito a portas com alto risco	O EC2.19 verifica se o tráfego de entrada irrestrito para um grupo de segurança está acessível às portas especificadas que são consideradas de alto risco. O Security Hub atualizou esse controle para contabilizar as listas de prefixos gerenciadas quando elas forem fornecidas como fonte para uma regra de grupo de segurança. O controle produzirá uma descoberta `FAILED` se as listas de prefixos contiverem as cadeias de caracteres '0.0.0.0/0' ou '::/0'.

Data da mudança	Título e ID do controle	Descrição de alteração
16 de novembro de 2023	[CloudWatch.15] CloudWatch os alarmes devem ter ações especificadas configuradas	O título de controle alterado de CloudWatch alarmes deve ter uma ação configurada para o estado ALARME e CloudWatch os alarmes devem ter ações especificadas configuradas.
16 de novembro de 2023	[CloudWatch.16] os grupos de CloudWatch registros devem ser mantidos por um período de tempo especificado	O título de controle alterado dos grupos de CloudWatch registros deve ser mantido por pelo menos 1 ano; os grupos de CloudWatch registros devem ser mantidos por um período de tempo especificado.
16 de novembro de 2023	[Lambda.5] As funções do Lambda da VPC devem operar em várias zonas de disponibilidade	Título de controle alterado de As funções do Lambda da VPC devem operar em mais de uma zona de disponibilidade para As funções do Lambda da VPC devem operar em várias zonas de disponibilidade.

Data da mudança	Título e ID do controle	Descrição de alteração
16 de novembro de 2023	[AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado	Título de controle alterado de O AWS AppSync ter o registro em log em nível de solicitação e em nível de campo ativado para O AWS AppSync deve ter o registro em log em nível de campo habilitado.
16 de novembro de 2023	[EMR.1] Os nós primários do cluster do Amazon EMR não devem ter endereços IP públicos	O título de controle alterado dos nós principais do MapReduce cluster Amazon Elastic não deve ter endereços IP públicos para os nós primários do cluster Amazon EMR não devem ter endereços IP públicos.
16 de novembro de 2023	Os OpenSearch domínios [Opensearch.2] não devem ser acessíveis ao público	O título de controle alterado dos OpenSearch domínios deve estar em uma VPC OpenSearch para que os domínios não possam ser acessíveis ao público.

Data da mudança	Título e ID do controle	Descrição de alteração
16 de novembro de 2023	[ES.2] Os domínios do Elasticsearch não devem ser publicamente acessíveis	Título de controle alterado de Os domínios do Elasticsearch devem estar em uma VPC para Os domínios do Elasticsearch não devem ser acessíveis publicamente.

Data da mudança	Título e ID do controle	Descrição de alteração
31 de outubro de 2023	[ES.4] O registro de erros do domínio Elasticsearch nos CloudWatch registros deve estar ativado	O ES.4 verifica se os domínios do Elasticsearch estão configurados para enviar registros de erro para o Amazon Logs. CloudWatch Anteriormente, o controle produziu uma PASSED descoberta para um domínio do Elasticsearch que tem todos os registros configurados para serem enviados ao CloudWatch Logs. O Security Hub atualizou o controle para produzir uma PASSED descoberta somente para um domínio do Elasticsearch configurado para enviar registros de erros para o Logs. CloudWatch O controle também foi atualizado para excluir as versões do Elasticsearch que não oferecem suporte a logs de erros da avaliação.

Data da mudança	Título e ID do controle	Descrição de alteração
16 de outubro de 2023	[EC2.13] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 22	O EC2.13 verifica se os grupos de segurança permitem acesso de entrada irrestrito à porta 22. O Security Hub atualizou esse controle para contabilizar as listas de prefixos gerenciadas quando elas forem fornecidas como fonte para uma regra de grupo de segurança. O controle produzirá uma descoberta `FAILED` se as listas de prefixos contiverem as cadeias de caracteres '0.0.0.0/0' ou '::/0'.

Data da mudança	Título e ID do controle	Descrição de alteração
16 de outubro de 2023	[EC2.14] Os grupos de segurança não devem permitir a entrada de 0.0.0.0/0 ou ::/0 na porta 3389	O EC2.14 verifica se os grupos de segurança permitem acesso irrestrito à porta 3389. O Security Hub atualizou esse controle para contabilizar as listas de prefixos gerenciadas quando elas forem fornecidas como fonte para uma regra de grupo de segurança. O controle produzirá uma descoberta `FAILED` se as listas de prefixos contiverem as cadeias de caracteres '0.0.0.0/0' ou '::/0'.

Data da mudança	Título e ID do controle	Descrição de alteração
16 de outubro de 2023	Os grupos de segurança só devem permitir tráfego de entrada irrestrito para portas autorizadas	O EC2.18 verifica se os grupos de segurança em uso não permitem tráfego de entrada irrestrito. O Security Hub atualizou esse controle para contabilizar as listas de prefixos gerenciadas quando elas forem fornecidas como fonte para uma regra de grupo de segurança. O controle produzirá uma descoberta `FAILED` se as listas de prefixos contiverem as cadeias de caracteres '0.0.0.0/0' ou '::/0'.

Data da mudança	Título e ID do controle	Descrição de alteração
16 de outubro de 2023	[Lambda.2] As funções do devem usar os tempos de execução mais recentes	O Lambda.2 verifica se as configurações da AWS Lambda função para tempos de execução correspondem aos valores esperados definidos para os tempos de execução suportados em cada idioma. O Security Hub agora oferece suporte `python3.11` como parâmetro.
4 de outubro de 2023	[S3.7] Os buckets de uso geral do S3 devem usar a replicação entre regiões	O Security Hub adicionou o parâmetro `ReplicationType` com um valor de `CROSS-REGION` para garantir que os buckets S3 tenham a replicação entre regiões ativada em vez da replicação na mesma região.

Data da mudança	Título e ID do controle	Descrição de alteração
27 de setembro de 2023	Os clusters EKS devem ser executados em uma versão compatível do Kubernetes	O Security Hub atualizou a versão mais antiga compatível do Kubernetes na qual o cluster Amazon EKS pode ser executado para produzir uma descoberta aprovada. A versão atual mais antiga compatível é o Kubernetes `1.24`.
20 de setembro de 2023	CloudFront.2 — CloudFront as distribuições devem ter a identidade de acesso de origem habilitada	O Security Hub descontinuou esse controle e o removeu de todos os padrões. Em vez disso, consulte [CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem. O controle de acesso à origem é a prática recomendada de segurança atual. Esse controle será removido da documentação em 90 dias.

Data da mudança	Título e ID do controle	Descrição de alteração
20 de setembro de 2023	[PCI.EC2.3] Os grupos de segurança do Amazon EC2 devem ser removidos	O Security Hub removeu esse controle do AWS Foundational Security Best Practices (FSBP) e do National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5. Ainda faz parte do Service-Managed Standard:. AWS Control Tower Esse controle da produz uma descoberta aprovada se os grupos de segurança estiverem conectado s a instâncias do EC2 ou a uma interface de rede elástica. Entretanto, para determinados casos de uso, grupos de segurança independe ntes não represent am um risco de segurança. É possível usar outros controles do EC2, como EC2.2, EC2.13, EC2.14, EC2.18 e EC2.19,

Data da mudança	Título e ID do controle	Descrição de alteração
		para monitorar seus grupos de segurança.
20 de setembro de 2023	EC2.29 — As instâncias do EC2 devem ser lançadas em uma VPC	O Security Hub descontinuou esse controle e o removeu de todos os padrões. O Amazon EC2 migrou instância s do EC2-Class ic para uma VPC. Esse controle será removido da documentação em 90 dias.

Data da mudança	Título e ID do controle	Descrição de alteração
20 de setembro de 2023	S3.4 – Os buckets do S3 devem ter a criptografia no lado do servidor habilitada	O Security Hub descontinuou esse controle e o removeu de todos os padrões. O Amazon S3 agora fornece criptografia padrão com chaves gerenciadas pelo S3 (SS3-S3) em buckets do S3 novos e existentes. As configurações de criptografia permanecem inalteradas para buckets existentes que são criptografados com criptografia SS3-S3 ou SS3-KMS do lado do servidor. Esse controle será removido da documentação em 90 dias.

Data da mudança	Título e ID do controle	Descrição de alteração
14 de setembro de 2023	[EC2.2] O grupo de segurança padrão da VPC não deve permitir o tráfego de entrada e saída	Título de controle alterado de O grupo de segurança padrão da VPC não deve permitir tráfego de entrada e saída para Os grupos de segurança padrão da VPC não devem permitir tráfego de entrada ou saída.
14 de setembro de 2023	[IAM.6] A MFA de hardware deve estar habilitada para o usuário raiz	Título de controle alterado de Virtual MFA deve ser habilitado para o usuário raiz para MFA deve ser habilitado para o usuário raiz.
14 de setembro de 2023	As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de cluster	Título de controle alterado de Uma assinatura de notificações de eventos do RDS deve ser configurada para eventos críticos do cluster para As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos do cluster.

Data da mudança	Título e ID do controle	Descrição de alteração
14 de setembro de 2023	As assinaturas existentes de notificação de eventos do RDS devem ser configuradas para eventos críticos de cluster	Título de controle alterado de Uma assinatura de notificações de eventos RDS deve ser configurada para eventos críticos de instância de banco de dados para Assinaturas de notificação de eventos RDS existentes devem ser configuradas para eventos críticos de instância de banco de dados.
14 de setembro de 2023	[WAF.2] As regras regionais AWS WAF clássicas devem ter pelo menos uma condição	Título de controle alterado de Uma regra regional do WAF deve ter pelo menos uma condição para as regras regionais clássicas do AWS WAF devem ter pelo menos uma condição.

Data da mudança	Título e ID do controle	Descrição de alteração
14 de setembro de 2023	[WAF.3] Os grupos de regras regionais AWS WAF clássicos devem ter pelo menos uma regra	Título de controle alterado de Um grupo de regras regionais do WAF deve ter pelo menos uma regra para grupos de regras regionais clássicas AWS WAF devem ter pelo menos uma regra.
14 de setembro de 2023	[WAF.4] As ACLs regionais AWS WAF clássicas da web devem ter pelo menos uma regra ou grupo de regras	Título de controle alterado de Uma ACL da web regional do WAF deve ter pelo menos uma regra ou grupo de regras para ACLs da web regionais clássicas do AWS WAF devem ter pelo menos uma regra ou grupo de regras.
14 de setembro de 2023	[WAF.6] As regras globais AWS WAF clássicas devem ter pelo menos uma condição	Título de controle alterado de Uma regra global do WAF deve ter pelo menos uma condição para As regras globais clássicas do AWS WAF devem ter pelo menos uma condição.

Data da mudança	Título e ID do controle	Descrição de alteração
14 de setembro de 2023	[WAF.7] Os grupos de regras globais AWS WAF clássicos devem ter pelo menos uma regra	Título de controle alterado de Um grupo de regras globais do WAF deve ter pelo menos uma regra para grupos de regras globais clássicas do AWS WAF devem ter pelo menos uma regra.
14 de setembro de 2023	[WAF.8] As ACLs web globais AWS WAF clássicas devem ter pelo menos uma regra ou grupo de regras	Título de controle alterado de Uma ACL da Web global do WAF deve ter pelo menos uma regra ou grupo de regras para ACLs da Web globais clássicas do AWS WAF devem ter pelo menos uma regra ou grupo de regras.
14 de setembro de 2023	[WAF.10] as ACLs AWS WAF da web devem ter pelo menos uma regra ou grupo de regras	Título de controle alterado de Uma ACL da web do WAFv2 deve ter pelo menos uma regra ou grupo de regras para as ACLs da web do AWS WAF devem ter pelo menos uma regra ou grupo de regras.

Data da mudança	Título e ID do controle	Descrição de alteração
14 de setembro de 2023	[WAF.11] O registro de ACL AWS WAF da web deve estar ativado	Título de controle alterado de ACL da web v2 do AWS WAF deve ser ativada para o logging de ACL da web do AWS WAF deve ser ativado.
20 de julho de 2023	S3.4 – Os buckets do S3 devem ter a criptografia no lado do servidor habilitada	S3.4 verifica se um bucket do Amazon S3 tem criptografia no lado do servidor habilitada ou se a política do bucket do S3 nega explicitamente solicitações do `PutObject` sem criptografia no lado do servidor. O Security Hub atualizou esse controle para incluir criptografia no lado do servidor de camada dupla com chaves KMS (DSSE-KMS). O controle produzirá uma descoberta aprovada quando um bucket do S3 for criptografado com SSE-S3, SSE-KMS ou DSSE-KMS.

Data da mudança	Título e ID do controle	Descrição de alteração
17 de julho de 2023	[S3.17] Os buckets de uso geral do S3 devem ser criptografados em repouso com AWS KMS keys	O S3.17 verifica se um bucket do Amazon S3 está criptografado com um AWS KMS key. O Security Hub atualizou esse controle para incluir criptografia no lado do servidor de camada dupla com chaves KMS (DSSE-KMS). O controle produzirá uma descoberta aprovada quando um bucket do S3 for criptografado com SSE-KMS ou DSSE-KMS.
9 de junho de 2023	Os clusters EKS devem ser executados em uma versão compatível do Kubernetes	O EKS.2 verifica se um cluster Amazon EKS está sendo executado em uma versão compatível do Kubernetes. A versão mais antiga compatível agora é `1.23`.

Data da mudança	Título e ID do controle	Descrição de alteração
9 de junho de 2023	[Lambda.2] As funções do devem usar os tempos de execução mais recentes	O Lambda.2 verifica se as configurações da AWS Lambda função para tempos de execução correspondem aos valores esperados definidos para os tempos de execução suportados em cada idioma. O Security Hub agora oferece suporte `ruby3.2` como parâmetro.
5 de junho de 2023	Os dados do cache da API REST de Gateway devem ser criptografados em repouso	APIgateway.5. verifica se todos os métodos nos estágios da API REST do Amazon API Gateway estão criptografados em repouso. O Security Hub atualizou o controle para avaliar a criptografia de um método específico somente quando o armazenamento em cache estiver habilitado para esse método.

Data da mudança	Título e ID do controle	Descrição de alteração
18 de maio de 2023	[Lambda.2] As funções do devem usar os tempos de execução mais recentes	O Lambda.2 verifica se as configurações da AWS Lambda função para tempos de execução correspondem aos valores esperados definidos para os tempos de execução suportados em cada idioma. O Security Hub agora oferece suporte `java17` como parâmetro.
18 de maio de 2023	[Lambda.2] As funções do devem usar os tempos de execução mais recentes	O Lambda.2 verifica se as configurações da AWS Lambda função para tempos de execução correspondem aos valores esperados definidos para os tempos de execução suportados em cada idioma. O Security Hub não é mais compatível com `nodejs12.x` como parâmetro.

Data da mudança	Título e ID do controle	Descrição de alteração
23 de abril de 2023	Os serviços ECS Fargate devem ser executados na versão mais recente da plataforma Fargate	O ECS.10 verifica se os serviços do Amazon ECS Fargate estão executando a versão da plataforma Fargate mais recente. Os clientes podem implantar o Amazon ECS por meio do ECS diretamente ou usando. CodeDeploy O Security Hub atualizou esse controle para produzir descobertas aprovadas quando você usa CodeDeploy para implantar serviços ECS Fargate.

Data da mudança	Título e ID do controle	Descrição de alteração
20 de abril de 2023	[S3.6] As políticas de bucket de uso geral do S3 devem restringir o acesso a outros Contas da AWS	O S3.6 verifica se uma política de bucket do Amazon Simple Storage Service (Amazon S3) impede que entidades principais de Contas da AWS terceiros executem ações negadas em recursos no bucket do S3. O Security Hub atualizou o controle para considerar as condicionais em uma política de bucket.
18 de abril de 2023	[Lambda.2] As funções do devem usar os tempos de execução mais recentes	O Lambda.2 verifica se as configura ções da AWS Lambda função para tempos de execução correspondem aos valores esperados definidos para os tempos de execução suportados em cada idioma. O Security Hub agora oferece suporte `python3.10` como parâmetro.

Data da mudança	Título e ID do controle	Descrição de alteração
18 de abril de 2023	[Lambda.2] As funções do devem usar os tempos de execução mais recentes	O Lambda.2 verifica se as configurações da AWS Lambda função para tempos de execução correspondem aos valores esperados definidos para os tempos de execução suportados em cada idioma. O Security Hub não é mais compatível com `dotnetcore3.1` como parâmetro.

Data da mudança	Título e ID do controle	Descrição de alteração
17 de abril de 2023	As instâncias do RDS devem ter backups automáticos habilitados	O RDS.11 verifica se as instâncias do Amazon RDS têm backups automatizados habilitados, com um período de retenção de backup maior ou igual a sete dias. O Security Hub atualizou esse controle para excluir réplicas de leitura da avaliação, pois nem todos os mecanismos oferecem suporte a backups automatizados em réplicas de leitura. Além disso, o RDS não oferece a opção de especificar um período de retenção de backup ao criar réplicas de leitura. As réplicas de leitura são criadas com um período de retenção de backup de `0` por padrão.

Histórico de documentos do Guia do Usuário do AWS Security Hub

A tabela a seguir descreve as atualizações na documentação do AWS Security Hub.

> **Note**
>
> Para lançamentos de controle de segurança, a data especificada é a data em que os controles estão disponíveis em todas as contas e regiões. Pode levar de 1 a 2 semanas para que os controles cheguem a todas as contas e regiões.

Alteração	Descrição	Data
Lançamento do CIS AWS Foundations Benchmark v3.0.0	O Security Hub lançou o Center for Internet Security (CIS) AWS Foundations Benchmark v3.0.0. A versão inclui os seguintes novos controles, bem como mapeamentos para vários controles existentes. • the section called “[EC2.53] Os grupos de segurança do EC2 não devem permitir a entrada de 0.0.0.0/0 nas portas de administração remota do servidor” • the section called “[EC2.54] Os grupos de segurança do EC2 não devem permitir a entrada de: :/0 nas portas de administração do servidor remoto”	13 de maio de 2024

- the section called “[IAM.26] Certificados SSL/TLS expirados gerenciados no IAM devem ser removidos”
- the section called “[IAM.27] As identidades do IAM não devem ter a política anexada AWSCloudShellFullAccess ”
- the section called “[IAM.28] O analisador de acesso externo do IAM Access Analyzer deve estar ativado”
- the section called “[S3.22] Os buckets de uso geral do S3 devem registrar eventos de gravação em nível de objeto”
- the section called “[S3.23] Os buckets de uso geral do S3 devem registrar eventos de leitura em nível de objeto”

Novos controles de segurança	Os seguintes novos controles do Security Hub estão disponíveis: • the section called “[DataFirehose.1] Os fluxos de entrega do Firehose devem ser criptografados em repouso” • the section called “[DMS.10] Os endpoints do DMS para bancos de dados Neptune devem ter a autorização do IAM habilitada” • the section called “[DMS.11] Os endpoints DMS para MongoDB devem ter um mecanismo de autenticação habilitado” • the section called “[DMS.12] Os endpoints DMS para Redis devem ter o TLS ativado” • the section called “[DynamoDB.7] Os clusters do DynamoDB Accelerator devem ser criptografados em trânsito” • the section called “[EFS.6] Os destinos de montagem do EFS não devem ser associados a uma sub-rede pública” • the section called “[EKS.3] Os clusters EKS devem	3 de maio de 2024

usar segredos criptografados do Kubernetes”

- the section called “[FSX.2] Os sistemas de arquivos FSx for Lustre devem ser configurados para copiar tags para backups”
- the section called “[MQ.2] Os corretores do ActiveMQ devem transmitir os registros de auditoria para CloudWatch”
- the section called “[MQ.3] Os corretores do Amazon MQ devem ter a atualização automática de versões secundárias ativada”
- the section called “Os OpenSearch domínios [Opensearch.11] devem ter pelo menos três nós primários dedicados”
- the section called “[Redshift.15] Os grupos de segurança do Redshift devem permitir a entrada na porta do cluster somente de origens restritas”
- the section called “[SageMaker.4] As variantes de produção de SageMaker endpoints devem ter uma contagem inicial de instâncias maior que 1”

	• the section called “[Service Catalog.1] Os portfólios do Service Catalog devem ser compartilhados somente dentro de uma organização AWS” • the section called “[Transfer.2] Os servidores Transfer Family não devem usar o protocolo FTP para conexão de endpoints”	
AWS Padrão de marcação de recursos	O AWS Resource Tagging Standard do Security Hub agora está disponível ao público em geral, junto com novos controles que se aplicam ao padrão.	30 de abril de 2024
Atualização da política gerenciada existente	O Security Hub atualizou a política AWS gerenciada nomeada `AmazonSecurityHubFullAccess` para obter detalhes de preços Serviços da AWS e produtos.	24 de abril de 2024
Configuração contextual dos parâmetros de controle	Se você usa a configuração central, agora você pode configurar os parâmetros de controle no contexto, na página de detalhes de um controle no console do Security Hub.	29 de março de 2024

Atualização da política gerenciada existente	O Security Hub atualizou a política AWS gerenciada nomeada `AWSSecurityHubReadOnlyAccess` adicionando um `Sid` campo.	22 de fevereiro de 2024
Novo controle de segurança	O controle [Macie.2] A descoberta automatizada de dados confidenciais do Macie deve ser ativada já está disponível. Para ver os limites regionais desse controle, consulte Disponibilidade de controles por região.	19 de fevereiro de 2024
Security Hub disponível no Oeste do Canadá (Calgary)	O Security Hub agora está disponível no Oeste do Canadá (Calgary). Todos os atributos do Security Hub agora estão disponíveis nessa região, com exceção de determinados controles de segurança. Para obter mais informações, consulte Disponibilidade de controles por região.	20 de dezembro de 2023

Novos controles de segurança	Os seguintes novos controles do Security Hub estão disponíveis: • the section called “[Backup. 1] os pontos de AWS Backup recuperação devem ser criptografados em repouso” • the section called “[DynamoDB.6] As tabelas do DynamoDB devem ter a proteção contra exclusão habilitada” • the section called “[EC2.51] Os endpoints da Client VPN do EC2 devem ter o registro em log de conexão do cliente habilitado” • the section called “[EKS.8] Os clusters do EKS devem ter o registro em log de auditoria habilitado” • the section called “[EMR.2] A configuração de bloqueio de acesso público do Amazon EMR deve estar habilitada” • the section called “[FSx.1] Os sistemas de arquivos do Amazon FSx para OpenZFS devem estar configura dos para copiar tags para backups e volumes.”	14 de dezembro de 2023

- the section called “[Macie.1] O Amazon Macie deve estar ativado”
- the section called “[MSK.2] Os clusters do MSK devem ter monitoramento aprimorado configurado”
- the section called “[Neptune.9] Os clusters de banco de dados do Neptune devem ser implantados em várias zonas de disponibilidade”
- the section called “[Network Firewall.1] Os firewalls do Network Firewall devem ser implantados em várias zonas de disponibilidade”
- the section called “[Network Firewall.2] O registro do Firewall de Rede deve estar ativado”
- the section called “Os OpenSearch domínios [Opensearch.10] devem ter a atualização de software mais recente instalada”
- the section called “[PCA.1] a autoridade de certificação AWS Private CA raiz deve ser desativada”
- the section called “[S3.19] Os pontos de acesso do S3 devem ter configurações de bloqueio do acesso público habilitadas”

	• the section called “[S3.20] Os buckets de uso geral do S3 devem ter a exclusão de MFA habilitada”	
Enriquecimento de descobertas	O Security Hub adicionou os novos campos `AwsAccountName` de `ApplicationArn` descoberta e `ApplicationName` ao Formato AWS de descoberta de segurança (ASFF).	27 de novembro de 2023
Aprimoramentos no painel Resumo	Agora é possível acessar mais widgets do painel na página Resumo do console do Security Hub, salvar conjuntos de filtros do painel para se concentrar rapidamente em problemas de segurança específicos e personalizar o layout do painel.	27 de novembro de 2023
Configuração central	A configuração central agora está disponível. Com a configuração central, o administrador delegado do Security Hub pode configurar o Security Hub, os padrões e os controles em várias contas organizacionais, unidades organizacionais (OUs) e regiões.	27 de novembro de 2023

Atualizações da política gerenciada	O Security Hub adicionou novas permissões à política gerenciada `AWSSecurityHubServiceRolePolicy` que permitem que o Security Hub leia e atualize propriedades de controle de segurança personalizáveis.	26 de novembro de 2023
Parâmetros de controle personalizados	Agora é possível personalizar os valores dos parâmetros para controles selecionados do Security Hub. Isso pode tornar as descobertas de um controle específico mais relevantes para seus requisitos de negócios e expectativas de segurança.	26 de novembro de 2023
Atualizações das políticas gerenciadas	O Security Hub atualizou `AWSSecurityHubFullAccess` e `AWSSecurityHubOrganizationsAccess` gerenciou as políticas que permitem que você use, respectivamente, os recursos do Security Hub e a integração com AWS Organizations.	16 de novembro de 2023

Controles de segurança existentes adicionados ao Service-Managed Standard: AWS Control Tower	Os seguintes controles existentes do Security Hub foram adicionados ao Service-Managed Standard:. AWS Control Tower • ACM.2 • AppSync5. • CloudTrail.6 • DMS.9 • DocumentDB.3 • DynamoDB.3 • EC2.23 • EKS.1 • ElastiCache.3 • ElastiCache.4 • ElastiCache5. • ElastiCache.6 • EventBridge.3 • KMS.4 • Lambda.3 • MQ.5 • MQ.6 • MSK.1 • RDS.12 • RDS.15 • S3.17	14 de novembro de 2023

Atualizações na política gerenciada	O Security Hub adicionou uma nova permissão de marcação para a política gerenciada `AWSSecurityHubServiceRolePolicy` que permite ao Security Hub ler tags de recursos relacionadas às descobertas.	7 de novembro de 2023

Novos controles de segurança	Os seguintes novos controles do Security Hub estão disponíveis: • the section called “[AppSync .5] As APIs AWS AppSync do GraphQL não devem ser autenticadas com chaves de API” • the section called “As instâncias de replicação do DMS devem ter a atualizaç ão automática de versões secundárias habilitada” • the section called “As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado” • the section called “As tarefas de replicação do DMS para o banco de dados de destino devem ter o registro em log ativado” • the section called “Os endpoints do DMS devem usar SSL” • the section called “Os instantâneos manuais do cluster do Amazon DocumentDB não devem ser públicos” • the section called “[DocumentDB.4] Os clusters do Amazon	10 de outubro de 2023

DocumentDB devem publicar registros de auditoria no Logs CloudWatch ”

- the section called “Os clusters do Amazon DocumentDB devem ter a proteção contra exclusão ativada”
- the section called “As definições de tarefas do ECS devem ter uma configuração de registro em log”
- the section called “[EventBridge.3] os ônibus de eventos EventBridge personalizados devem ter uma política baseada em recursos anexada”
- the section called “[EventBridge.4] endpoints EventBridge globais devem ter a replicação de eventos ativada”
- the section called “Os clusters MSK devem ser criptografados em trânsito entre os nós do agente”
- the section called “Os agentes do ActiveMQ devem usar o modo de implantação ativo/em espera”

- the section called “Os agentes do RabbitMQ devem usar o modo de implantação de cluster”
- the section called “[Network Firewall.9] Os firewalls do Firewall de Rede devem ter a proteção contra exclusão ativada”
- the section called “[RDS.34] Os clusters de banco de dados Aurora MySQL devem publicar registros de auditoria no Logs CloudWatch ”
- the section called “Os clusters de banco de dados do RDS devem ter a atualização automática de versões secundárias ativada”
- the section called “As zonas hospedadas públicas do Route 53 devem registrar consultas de DNS”
- the section called “As AWS WAF regras [WAF.12] devem ter métricas habilitadas CloudWatch ”

Atualizações na política gerenciada	O Security Hub adicionou novas ações do Organizations à política gerenciada `AWSSecurityHubServiceRolePolicy` que permitem que o Security Hub recupere informações da conta e da unidade organizacional (OU). Também foram adicionadas novas ações do Security Hub que permitem que o Security Hub leia e atualize as configurações do serviço, incluindo padrões e controles.	27 de setembro de 2023

Controles de segurança existentes adicionados ao Service-Managed Standard: AWS Control Tower	Os seguintes controles existentes do Security Hub foram adicionados ao Service-Managed Standard:. AWS Control Tower • the section called “Os grupos de trabalho do Athena devem ser criptografados em repouso” • the section called “Os clusters do Amazon DocumentDB devem ser criptografados em repouso” • the section called “Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado” • the section called “Os clusters de banco de dados Neptune devem ser criptografados em repouso” • the section called “[Neptune .2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch ” • the section called “Os instantâneos do cluster de banco de dados Neptune não devem ser públicos” • the section called “[Neptune .4] Os clusters de banco de	26 de setembro de 2023

dados Neptune devem ter a proteção contra exclusão ativada”

- the section called “Os clusters de banco de dados Neptune devem ter backups automatizados habilitados”
- the section called “Os clusters de banco de dados Neptune devem ser criptografados em repouso”
- the section called “[Neptune .7] Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada”
- the section called “Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos”
- the section called “Os clusters de banco de dados Neptune devem ser criptografados em repouso”

Visualização de controles consolidados e resultados de controle consolidados disponíveis em AWS GovCloud (US)	A visualização dos controles consolidados e as descobertas dos controles consolidados agora estão disponíveis no AWS GovCloud (US) Region. A página Controles do console do Security Hub mostra todos os seus controles em todos os padrões. Cada controle tem a mesma ID de controle em todos os padrões. Ao ativar as descobertas de controle consolidadas, você recebe uma única descoberta por verificação de segurança, mesmo quando um controle se aplica a vários padrões habilitados.	6 de setembro de 2023

Visualização de controles consolidados e descobertas de controle consolidadas disponíveis nas regiões da China	A visualização dos controles consolidados e as descobertas dos controles consolidados agora estão disponíveis nas regiões da China. A página Controles do console do Security Hub mostra todos os seus controles em todos os padrões. Cada controle tem a mesma ID de controle em todos os padrões. Ao ativar as descobertas de controle consolidadas, você recebe uma única descoberta por verificação de segurança, mesmo quando um controle se aplica a vários padrões habilitados.	28 de agosto de 2023
Security Hub disponível na região de Israel (Tel Aviv)	O Security Hub já está disponível em Israel (Tel Aviv). Todos os atributos do Security Hub agora estão disponíveis nessa região, com exceção de determinados controles de segurança. Para obter mais informações, consulte Disponibilidade de controles por região.	8 de agosto de 2023

Novos controles de segurança	Os seguintes novos controles do Security Hub estão disponíveis: • the section called “Os grupos de trabalho do Athena devem ser criptografados em repouso” • the section called “Os clusters do Amazon DocumentDB devem ser criptografados em repouso” • the section called “Os clusters do Amazon DocumentDB devem ter um período de retenção de backup adequado” • the section called “Os clusters de banco de dados Neptune devem ser criptografados em repouso” • the section called “[Neptune .2] Os clusters de banco de dados Neptune devem publicar registros de auditoria no Logs CloudWatch ” • the section called “Os instantâneos do cluster de banco de dados Neptune não devem ser públicos” • the section called “[Neptune .4] Os clusters de banco de dados Neptune devem ter	28 de julho de 2023

	a proteção contra exclusão ativada” • the section called “Os clusters de banco de dados Neptune devem ter backups automatizados habilitados” • the section called “Os clusters de banco de dados Neptune devem ser criptografados em repouso” • the section called “[Neptune .7] Os clusters de banco de dados Neptune devem ter a autenticação de banco de dados do IAM habilitada” • the section called “Os clusters de banco de dados Neptune devem ser configurados para copiar tags para instantâneos” • the section called “Os clusters de banco de dados Neptune devem ser criptografados em repouso”	
Novos operadores para critérios de regras de automação	Agora, você pode usar os operadores de comparação CONTAINS e NOT_CONTAINS para mapa de regras de automação e critérios de string.	25 de julho de 2023

Regras de automação	O Security Hub agora oferece regras de automação que atualizam descobertas automaticamente com base nos critérios especificados.	13 de junho de 2023
Novas integrações de terceiros	O Snyk é uma nova integraçã o de terceiros que envia as descobertas para o Security Hub.	12 de junho de 2023

Controles de segurança existentes adicionados ao Service-Managed Standard: AWS Control Tower	Os seguintes controles existentes do Security Hub foram adicionados ao Service-Managed Standard:. AWS Control Tower • the section called “[Conta.1] As informações de contato de segurança devem ser fornecidas para um Conta da AWS” • the section called “As rotas do API de Gateway devem especificar um tipo de autorização” • the section called “O registro de acesso deve ser configurado para os estágios V2 do API de Gateway” • the section called “[CodeBuild.3] Os registros do CodeBuild S3 devem ser criptografados” • the section called “Os modelos de lançamento do Amazon EC2 não devem atribuir IPs públicos às interfaces de rede” • the section called “[ELBv2.1] O Application Load Balancer deve ser configurado para redirecionar todas as solicitações HTTP para HTTPS”	12 de junho de 2023

- the section called “[Redshift.10] Os clusters do Redshift devem ser criptografados em repouso”
- the section called “[SageMaker.2] as instâncias do SageMaker notebook devem ser iniciadas em uma VPC personalizada”
- the section called “[SageMaker.3] Os usuários não devem ter acesso root às instâncias do SageMaker notebook”
- the section called “[WAF.10] as ACLs AWS WAF da web devem ter pelo menos uma regra ou grupo de regras”

Novos controles de segurança	Os seguintes novos controles do Security Hub estão disponíveis: • the section called “Os certificados RSA gerenciados pelo ACM devem usar um comprimento de chave de pelo menos 2.048 bits” • the section called “[AppSync.2] AWS AppSync deve ter o registro em nível de campo ativado” • the section called “[CloudFront.13] CloudFront as distribuições devem usar o controle de acesso de origem” • the section called “[Elastic Beanstalk.3] O Elastic Beanstalk deve transmitir registros para CloudWatch” • the section called “[S3.17] Os buckets de uso geral do S3 devem ser criptografados em repouso com AWS KMS keys” • the section called “[StepFunctions.1] As máquinas de estado do Step Functions devem ter o registro ativado”	6 de junho de 2023

Security Hub disponível na Ásia-Pacífico (Melbourne)	O Security Hub já está disponível na região Ásia-Pacífico (Melbourne). Todos os atributos do Security Hub agora estão disponíveis nessa região, com exceção de determinados controles de segurança. Para obter mais informações, consulte Disponibilidade de controles por região.	25 de maio de 2023
Histórico de descobertas	O Security Hub agora pode rastrear o histórico de uma descoberta durante os últimos 90 dias.	4 de maio de 2023

Novos controles de segurança	Os seguintes novos controles do Security Hub estão disponíveis: • the section called “Os endpoints do cluster EKS não devem ser acessíveis ao público” • the section called “[ELB.16] Os balanceadores de carga de aplicativos devem ser associados a uma ACL da web AWS WAF” • the section called “[Redshift.10] Os clusters do Redshift devem ser criptografados em repouso” • the section called “[S3.15] Os buckets de uso geral do S3 devem ter o Object Lock ativado”	29 de março de 2023
Suporte expandido para descobertas de controle consolidadas	O Automated Security Response na AWS v2.0.0 agora oferece suporte a descobertas de controle consolidadas.	24 de março de 2023
Security Hub disponível em novo Regiões da AWS	O Security Hub já está disponível na região Ásia-Pacífico (Hyderabad), Europa (Espanha) e Europa (Zurique). Há limites relacionados aos controles disponíveis nessas regiões.	21 de março de 2023

Política gerenciada atualizada	O Security Hub atualizou uma permissão existente na política gerenciada `AWSSecurityHubServiceRolePolicy` .	17 de março de 2023

Novos controles de segurança para o padrão NIST 800-53	O Security Hub adicionou os seguintes controles de segurança, que são aplicáveis ao padrão NIST 800-53: • the section called “[Aconta.2] Contas da AWS deve fazer parte de uma organização AWS Organizations” • the section called “[CloudWatch.15] CloudWatch os alarmes devem ter ações especificadas configuradas” • the section called “[CloudWatch.16] os grupos de CloudWatch registros devem ser mantidos por um período de tempo especificado” • the section called “[CloudWatch.17] ações de CloudWatch alarme devem ser ativadas” • the section called “As tabelas do DynamoDB devem estar presentes em um plano de backup” • the section called “[EC2.28] Os volumes do EBS devem ser cobertos por um plano de backup” • EC2.29: as instâncias do EC2 devem ser iniciadas em uma VPC (descontinuado)	3 de março de 2023

	• the section called “As instâncias de banco de dados do RDS devem ser protegidas por um plano de backup” • the section called “[S3.14] Os buckets de uso geral do S3 devem ter o controle de versão ativado” • the section called “[WAF.11] O registro de ACL AWS WAF da web deve estar ativado”	
Instituto Nacional de Padrões e Tecnologia (National Institute of Standards and Technology, NIST) 800-53 Revisão 5	O Security Hub agora oferece suporte ao padrão NIST 800-53 Rev. 5 com mais de 200 controles de segurança aplicáveis.	28 de fevereiro de 2023
Visualização de controles consolidados e descobertas de controle	Com o lançamento da visualização de controles consolidados, a página Controles do console do Security Hub mostra todos os seus controles em todos os padrões. Cada controle tem a mesma ID de controle em todos os padrões. Ao ativar as descobertas de controle consolidadas, você recebe uma única descoberta por verificação de segurança, mesmo quando um controle se aplica a vários padrões habilitados.	23 de fevereiro de 2023

Novos controles de segurança	Os seguintes novos controles do Security Hub estão disponíveis. Alguns controles têm limitações regionais. • the section called “[ElastiCache.1] Os clusters ElastiCache Redis devem ter o backup automático ativado” • the section called “[ElastiCache.2] ElastiCache para clusters de cache Redis deve ter a atualização automática de versão secundária habilitada” • the section called “[ElastiCache.3] ElastiCache para grupos de replicação do Redis, o failover automático deve estar ativado” • the section called “[ElastiCache.4] ElastiCache para Redis, os grupos de replicação devem ser criptografados em repouso” • the section called “[ElastiCache.5] ElastiCache para Redis, os grupos de replicação devem ser criptografados em trânsito” • the section called “[ElastiCache.6] ElastiCache para grupos de replicação do	16 de fevereiro de 2023

	Redis antes da versão 6.0 deve usar o Redis AUTH” • the section called “[ElastiCache.7] os ElastiCache clusters não devem usar o grupo de sub-rede padrão”	
Novos campos do ASFF	O Security Hub foi adicionado o ProductFields. ArchivalReasons:0/Descrição e. ProductFields ArchivalReasons:0/ ReasonCode para o AWS Security Finding Format (ASFF).	8 de fevereiro de 2023
Novos campos do ASFF	O Security Hub adicionou conformidade. AssociatedStandards e conformidade. SecurityControlId para o AWS Security Finding Format (ASFF).	31 de janeiro de 2023
Os detalhes da vulnerabilidade já estão disponíveis	Agora é possível ver os detalhes sobre vulnerabilidade no console do Security Hub e consultar as descobertas que o Amazon Inspector envia para o Security Hub.	14 de janeiro de 2023
O Security Hub está disponível no Oriente Médio (Emirados Árabes Unidos)	O Security Hub já está disponível no Oriente Médio (Emirados Árabes Unidos). Alguns controles têm limites regionais.	12 de janeiro de 2023

Adicionada a integração de terceiros com o MetricStream	O Security Hub agora oferece suporte a uma integração de terceiros MetricStream em todas as regiões, exceto na China AWS GovCloud (US) e.	11 de janeiro de 2023
Aumento do limite da conta organizacional	O Security Hub agora é compatível com até 11.000 contas-membro para cada conta de administrador do Security Hub por região.	27 de dezembro de 2022
ElasticBeanstalk.3 Revertido	O Security Hub reverteu o controle [ElasticBeanstalk. 3] O Elastic Beanstalk deve transmitir CloudWatch registros do padrão FSBP em todas as regiões.	21 de dezembro de 2022
O Security Hub adiciona novos controles de segurança	Os novos controles do Security Hub estão disponíve is para clientes que habilitar am o padrão FSBP. Alguns controles têm limitações regionais.	15 de dezembro de 2022
Orientações sobre os próximos atributos	O Security Hub planeja lançar dois novos atributos: visualiza ção de controles consolida dos e descobertas de controle consolidadas. Esses atributos futuros podem afetar os fluxos de trabalho existentes que dependem do controle para localizar campos e valores.	9 de dezembro de 2022

A integração do Amazon Security Lake já está disponível	O Security Lake agora se integra ao Security Hub ao receber as descobertas do Security Hub.	29 de novembro de 2022
Support for Service-Managed Standard: AWS Control Tower	O Security Hub oferece suporte a um novo padrão de segurança chamado Service-Managed Standard:. AWS Control Tower AWS Control Tower gerencia esse padrão.	28 de novembro de 2022
O CIS AWS Foundations Benchmark v1.4.0 agora disponível nas regiões da China	O Security Hub agora oferece suporte ao CIS AWS Foundations Benchmark v1.4.0 nas regiões da China.	18 de novembro de 2022
A integração com o Jira Service Management Cloud já está disponível	O Jira Service Managemen t Cloud agora recebe as descobertas do Security Hub em todas as regiões disponíve is, exceto nas regiões da China.	17 de novembro de 2022
AWS IoT Device Defender integração agora disponível	AWS IoT Device Defender agora envia as descobertas para o Security Hub em todas as regiões disponíveis.	17 de novembro de 2022
Support para o CIS AWS Foundations Benchmark v1.4.0	O Security Hub agora fornece controles de segurança compatíveis com o CIS AWS Foundations Benchmark v1.4.0. O padrão está disponível em todas as regiões, exceto nas regiões da China.	9 de novembro de 2022

Support para anúncios do Security Hub em AWS GovCloud (US)	Agora você pode assinar os anúncios do Security Hub com o Amazon Simple Notification Service (Amazon SNS) AWS GovCloud em (Leste dos EUA) AWS GovCloud e (Oeste dos EUA) para receber notificaç ões sobre o Security Hub.	3 de outubro de 2022
AWS Security Hub adiciona um novo controle de segurança	O novo Security Hub control AutoScaling.9 está disponíve l para clientes que habilitaram o padrão FSBP. Os controles podem ter limitações regionais .	1º de setembro de 2022
Assinar os anúncios do Security Hub	Agora é possível assinar os anúncios do Security Hub com o Amazon Simple Notification Service (Amazon SNS) para receber notificações sobre o Security Hub.	29 de agosto de 2022
Expansão da região para agregação entre regiões	A agregação entre regiões já está disponível para descobert as, atualizações e insights em todas as regiões AWS GovCloud (US).	2 de agosto de 2022
Novas integrações de produtos de terceiros	Fortinet – O FortiCNP é uma integração de terceiros que recebe as descobertas do Security Hub, e o JFrog é uma integração de terceiros que envia as descobertas para o Security Hub.	26 de julho de 2022

EC2.27 é descontinuado	O Security Hub retirou o EC2.27 — A execução de instâncias do EC2 não deve usar pares de chaves, um antigo controle no padrão AWS Foundational Security Best Practices (FSBP).	20 de julho de 2022
Lambda.2 não é mais compatível com o python3.6	O Security Hub não oferece mais suporte ao python3.6 como parâmetro para o Lambda.2 - As funções do Lambda devem usar tempos de execução compatíveis, um controle no padrão Foundatio nal Security Best Practices (FSBP). AWS	19 de julho de 2022
AWS O Security Hub adiciona novos controles de segurança	Os novos controles do Security Hub estão disponíve is para clientes que habilitar am o padrão FSBP. Alguns controles têm limitações regionais.	22 de junho de 2022
AWS O Security Hub oferece suporte a uma nova região	O Security Hub já está disponível na Ásia-Pacífico (Jacarta). Alguns controles não estão disponíveis nesta região.	7 de junho de 2022
Integração aprimorada entre o AWS Security Hub e AWS Config	Os usuários do Security Hub podem ver os resultados das avaliações de AWS Config regras como descobertas no Security Hub.	6 de junho de 2022

Adicionada capacidade de cancelar padrões habilitados automaticamente	Para usuários que se integraram ao AWS Organizations, esse recurso permite que você faça login na conta de administrador do Security Hub e exclua novas contas de membros dos padrões ativados automaticamente.	25 de abril de 2022
Agregação entre regiões expandida	Agregação entre regiões adicionada para controlar status e pontuações de segurança.	20 de abril de 2022
CompanyName e agora ProductName são atributos de nível superior	Foram adicionados novos atributos de nível superior para definir nomes de empresas e produtos associados a integrações personalizadas	1.º de abril de 2022
Foram adicionados novos controles ao padrão AWS Boundational Security Best Practices	Foram adicionados novos controles ao Padrão das melhores práticas de segurança básica da AWS	31 de março de 2022
Foram adicionados novos objetos de detalhes de recursos ao ASFF	Tipo de recurso `AwsRdsDbSecurityGroup` adicionado ao ASFF.	25 de março de 2022
Mais detalhes de recursos foram adicionados ao ASFF	Mais detalhes adicionados a `AwsAutoScalingScalingGroup` , `AwsElbLoadBalancer` , `AwsRedshiftCluster` e `AwsCodeBuildProject` .	25 de março de 2022

Foram adicionados novos controles ao padrão AWS Boundational Security Best Practices	Foram adicionados 15 novos controles ao Padrão das melhores práticas de segurança básica da AWS .	16 de março de 2022
Foram adicionados novos controles ao padrão de Boas Práticas AWS de Segurança Fundamental e ao Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS)	Foram adicionados novos controles para Amazon OpenSearch Service, Amazon RDS, Amazon EC2, Elastic Load Balancing e AWS ao padrão Foundational CloudFront Security Best Practices. Também foram adicionados dois novos controles de OpenSearch serviço ao PCI DSS.	15 de fevereiro de 2022
Novo campo adicionado ao ASFF	Novo campo adicionado: Amostra.	26 de janeiro de 2022
Integração adicional com AWS Health	AWS Health usa mensagens de service-to-service eventos para enviar descobertas ao Security Hub.	19 de janeiro de 2022
Integração adicional com AWS Trusted Advisor	Trusted Advisor envia os resultados de suas verificaç ões para o Security Hub como descobertas do Security Hub. O Security Hub envia os resultados de suas AWS verificações de melhores práticas de segurança básica para Trusted Advisor.	18 de janeiro de 2022

Objetos de detalhes de recursos atualizados no ASFF	`MixedInstancesPolicy` e `AvailabilityZones` adicionados a `AwsAutoScalingAutoScalingGroup` . adicionado a `.MetadataOptions` `AwsAutoScalingLaunchConfiguration` adicionado a `.BucketVersioningConfiguration` `AwsS3Bucket`	20 de dezembro de 2021
Saída atualizada para a documentação do ASFF	As descrições dos atributos do ASFF estavam anteriormente em um único tópico. Cada objeto de nível superior e cada objeto de detalhes do recurso agora estão em seu próprio tópico. O tópico de sintaxe do ASFF contém links para esses tópicos.	20 de dezembro de 2021
Foram adicionados novos objetos de detalhes de recursos ao ASFF para AWS Network Firewall	Para AWS Network Firewall, foram adicionados os seguintes objetos de detalhes do recurso: `AwsNetworkFirewallFirewall` `AwsNetworkFireFirewallPolicy` , `AwsNetworkFirewallRuleGroup` e.	20 de dezembro de 2021

Suporte adicionado à nova versão do Amazon Inspector	O Security Hub está integrado à nova versão do Amazon Inspector, bem como com o Amazon Inspector Classic. O Amazon Inspector envia as descobertas para o Security Hub.	29 de novembro de 2021
Alterada a gravidade do EC2.19	A gravidade do EC2.19 (Os grupos de segurança não devem permitir acesso irrestrito às portas com alto risco) foi alterada de Alta para Crítica.	17 de novembro de 2021
Nova integração com o Sonrai Dig	O Security Hub agora oferece uma integração com o Sonrai Dig. O Sonrai Digmonitora ambientes de nuvem para identificar riscos de segurança. O Sonrai Dig envia descobertas para o Security Hub.	12 de novembro de 2021
Verificação atualizada dos controles CIS 2.1 e CloudTrail 1.1	Além de verificar se pelo menos uma CloudTrail trilha multirregional está em vigor, o CIS 2.1 e CloudTrail .1 agora também verificam se o `ExcludeManagementEventSources` parâmetro está vazio em pelo menos uma das trilhas multirregionais. CloudTrail	9 de novembro de 2021
Suporte adicionado aos endpoints da VPC	O Security Hub agora está integrado AWS PrivateLink e oferece suporte a endpoints VPC.	3 de novembro de 2021

Controles adicionados ao padrão AWS Foundational Security Best Practices	Foram adicionados novos controles para o Elastic Load Balancing (ELB.2 e ELB.8) e (SSM.4). AWS Systems Manager	2 de novembro de 2021
Portas adicionadas à verificação do controle EC2.19	O EC2.19 agora também verifica se os grupos de segurança não permitem acesso de entrada irrestrito às seguintes portas: 3000 (estruturas de desenvolvimento web Go, Node.js e Ruby), 5000 (estruturas de desenvolvimento web Python), 8088 (porta HTTP legada) e 8888 (porta HTTP alternativa)	27 de outubro de 2021
Adicionada a integração com o Logz.io Cloud SIEM	A Logz.io é uma provedora de Cloud SIEM que fornece correlação avançada de dados de log e eventos para ajudar as equipes de segurança a detectar, analisar e responder a ameaças à segurança em tempo real. O Logz.io recebe todas as descobertas do Security Hub.	25 de outubro de 2021

Suporte adicionado à agregação entre regiões das descobertas	A agregação entre regiões permite que você visualize todas as suas descobert as sem precisar alterar as regiões. As contas de administrador escolhem uma região de agregação e regiões vinculadas. As descobertas da conta do administrador e de suas contas membros são agregadas das regiões vinculadas à região de agregação.	20 de outubro de 2021
Objetos de detalhes de recursos atualizados no ASFF	Detalhes do certificado de visualizador adicionados ao `AwsCloudFrontDistr ibution` . Mais detalhes foram adicionados a `AwsCodeBuildProjec t` . Atributos do balancead or de carga adicionados ao `AwsElbV2LoadBalancer` . O identificador da conta do proprietário do bucket S3 foi adicionado a `AwsS3Bucket` .	8 de outubro de 2021

Adicionados novos objetos de detalhes de recursos ao ASFF	Foram adicionados os seguintes novos objetos de detalhes do recurso ao ASFF: `AwsEc2VpcEndpointService` , `AwsEcrRepository` , `AwsEksCluster` , `AwsOpenSearchServiceDomain` , `AwsWafRateBasedRule` , `AwsWafRegionalRateBasedRule` e `AwsXrayEncryptionConfig`	8 de outubro de 2021
Runtime obsoleto removido do controle Lambda.2	No padrão AWS Foundational Security Best Practices , removido o `dotnetcore2.1` tempo de execução do [Lambda.2] As funções do Lambda devem usar tempos de execução compatíveis.	6 de outubro de 2021
Novo nome para integração com a Check Point	A integração com o Check Point Dome9 Arc agora é o Check Point CloudGuard Posture Management. O ARN de integração não mudou.	1.º de outubro de 2021
Integração com o Alcide removida	A integração com o Alcide KAudit foi descontinuada.	30 de setembro de 2021
Alterada a gravidade do EC2.19	A gravidade do [EC2.19] Os grupos de segurança não devem permitir acesso irrestrito às portas com alto risco foi alterada de Média para Alta.	30 de setembro de 2021

A integração com agora AWS Organizations é suportada nas regiões da China	Agora há suporte para a integração do Security Hub com o Organizations nas regiões China (Pequim) e China (Ningxia).	20 de setembro de 2021
Nova AWS Config regra para os controles S3.1 e PCI.S3.6	Tanto o S3.1 quanto o PCI.S3.6 verificam se a configuração do Bloqueio de Acesso Público do Amazon S3 está habilitada. A AWS Config regra para esses controles é alterada de `s3-account-level-public-access-blocks` para `s3-account-level-public-access-blocks-periodic` .	14 de setembro de 2021
Os runtimes obsoletos foram removidos do controle Lambda.2	No padrão AWS Foundational Security Best Practices , removido do `nodejs10.x` [Lambda.2], as funções do Lambda devem usar `ruby2.5` tempos de execução compatíveis.	13 de setembro de 2021
A gravidade do controle CIS 2.2 foi alterada	No padrão CIS AWS Foundations Benchmark, a severidade para 2.2. — A garantia de que a validação do arquivo de CloudTrail log está ativada foi alterada de Baixa para Média.	13 de setembro de 2021

ECS.1, Lambda.2 e SSM.1 atualizados no padrão Foundational Security Best Practices AWS	No padrão AWS Foundational Security Best Practices, o ECS.1 agora tem um `SkipInactiveTaskDefinitions` parâmetro definido como. `true` Isso garante que o controle verifique somente as definições de tarefas ativas. Para o Lambda.2, o Python 3.9 foi adicionado à lista de runtimes. O SSM.1 agora verifica as instâncias paradas e em execução.	7 de setembro de 2021
O controle PCI.Lambda.2 agora exclui os recursos do Lambda @Edge	No padrão Payment Card Industry Data Security Standard (PCI DSS), o controle PCI.Lambda.2 agora exclui os recursos do Lambda @Edge.	7 de setembro de 2021
Adicionada integração com o HackerOne Vulnerability Intelligence	O Security Hub agora oferece uma integração com o HackerOne Vulnerability Intelligence. A integração envia as descobertas para o Security Hub.	7 de setembro de 2021

Objetos de detalhes de recursos atualizados no ASFF	Para `AwsKmsKey`, foi adicionado `KeyRotationStatus`. Para `AwsS3Bucket`, `AccessControlList`, `BucketLoggingConfiguration`, `BucketNotificationConfiguration` e `BucketWebsiteConfiguration` foram adicionados.	2 de setembro de 2021
Adicionados novos objetos de detalhes de recursos ao ASFF	Foram adicionados os seguintes novos objetos de detalhes do recurso ao ASFF: `AwsAutoScalingLaunchConfiguration`, `AwsEc2VpnConnection` e `AwsEcrContainerImage`.	2 de setembro de 2021
Detalhes adicionados ao objeto `Vulnerabilities` no ASFF	Em `Cvss`, foram adicionados `Adjustments` e `Source`. Em `VulnerablePackages`, foram adicionados o caminho do arquivo e o gerenciador de pacotes.	2 de setembro de 2021
O Systems Manager Explorer e a OpsCenter integração agora são suportados nas regiões da China	A integração do Security Hub com o SSM Explorer agora OpsCenter é suportada na China (Pequim) e na China (Ningxia).	31 de agosto de 2021

Descontinuação do controle Lambda.4	O Security Hub está descontinuando o controle [Lambda.4] As funções do Lambda devem ter uma fila de mensagens não entregues configurada. Quando um controle é descontinuado, ele não é mais exibido no console e o Security Hub não executa verificações nele.	31 de agosto de 2021
Descontinuação do controle PCI.EC2.3	O Security Hub está descontinuando o controle [PCI.EC2.3] Os grupos de segurança do EC2 não utilizados devem ser removidos. Quando um controle é descontinuado, ele não é mais exibido no console e o Security Hub não executa verificações nele.	27 de agosto de 2021
Alteração na forma como o Security Hub envia as descobertas para ações personalizadas	Quando você envia as descobertas para uma ação personalizada, o Security Hub agora envia cada descoberta em um evento Security Hub Findings - Custom Actionseparado.	20 de agosto de 2021

Adicionado um novo código de motivo de status de conformidade para os runtimes personalizados do Lambda	Foi adicionado um novo código de motivo do status de conformidade `LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE` . Esse código de motivo indica que o Security Hub não pôde realizar uma verificação em um runtime do Lambda personalizado.	20 de agosto de 2021
AWS Firewall Manager integração agora suportada nas regiões da China	Agora há suporte para a integração do Security Hub com o Firewall Manager nas regiões China (Pequim) e China (Ningxia).	19 de agosto de 2021
Novas integrações com Caveonix Cloud e Forcepoint Cloud Security Gateway	O Security Hub agora oferece integrações com Caveonix Cloud e Forcepoint Cloud Security Gateway. Ambas as integrações enviam as descobertas para o Security Hub.	10 de agosto de 2021

Adicionados novos atributos `CompanyName` , `ProductName` e `Region` ao ASFF	Campos `CompanyName` , `ProductName` e `Region` adicionados ao nível superior do ASFF. Estes campos são preenchidos automaticamente e, exceto para integrações personalizadas de produtos, não podem ser atualizados usando `BatchImportFindings` ou `BatchUpdateFindings` . No console, os filtros de descobertas utilizam esses novos campos. Na API, os filtros `CompanyName` e `ProductName` usam os atributos que estão em `ProductFields` .	23 de julho de 2021
Objetos de detalhes de recursos adicionados e atualizados no ASFF	Adição de um novo tipo de recurso `AwsRdsEventSubscription` e de novos detalhes de recursos. Detalhes do recurso adicionados ao tipo de recurso `AwsEcsService` . Atributos adicionados ao objeto de detalhes do recurso `AwsElasticsearchDomain` .	23 de julho de 2021

Controles adicionados ao padrão AWS Foundational Security Best Practices	Foram adicionados novos controles para Amazon API Gateway (ApiGateway.5), Amazon EC2 (EC2.19), Amazon ECS (ECS.2), Elastic Load Balancing (ELB.7), Amazon Service (ES.5 a ES.8), Amazon RDS (RDS.16 a RDS.23), OpenSearch Amazon Redshift (Redshift.4) e Amazon SQS (SQS.1).	20 de julho de 2021
Movida uma permissão dentro da política gerenciada por função vinculada ao serviço	A permissão `config:PutEvaluations` foi movida dentro da política gerenciada `AWSSecurityHubServiceRolePolicy` para que ela seja aplicada a todos os recursos.	14 de julho de 2021
Controles adicionados ao padrão AWS Foundational Security Best Practices	Foram adicionados novos controles para Amazon API Gateway (ApiGateway.4), Amazon CloudFront (.5 e CloudFront .6), CloudFront Amazon EC2 (EC2.17 e EC2.18), Amazon ECS (ECS.1), Amazon Service AWS Identity and Access Management (ES.4), (IAM.21 OpenSearch), Amazon RDS (RDS.15) e Amazon S3 (S3.8).	8 de julho de 2021

Adicionados novos códigos de motivo do status de conformidade para as descobertas de controle	O `INTERNAL_SERVICE_ERROR` indica que ocorreu um erro desconhecido. O `SNS_TOPIC_CROSS_ACCOUNT` indica que o tópico do SNS pertence a uma conta diferente. O `SNS_TOPIC_INVALID` indica que o tópico SNS associado é inválido.	6 de julho de 2021
Adicionou a integração com AWS Chatbot	Foi adicionada a integração com AWS Chatbot. O Security Hub envia descobertas para AWS Chatbot.	30 de junho de 2021
Adicionada uma nova permissão à política gerenciada da função vinculada ao serviço	Adicionada uma nova permissão à política gerenciada `AWSSecurityHubServiceRolePolicy` para permitir que a função vinculada ao serviço forneça resultados de avaliação para AWS Config.	29 de junho de 2021
Objetos de detalhes de recursos novos e atualizados no ASFF	Foram adicionados novos objetos de detalhes de recursos aos clusters do ECS e definições de tarefas do ECS. Atualizado o objeto de instância EC2 para listar as interfaces de rede associadas. Adicionada a ID do certificado do cliente para os estágios da API Gateway V2. Adicionada a configuração do ciclo de vida dos buckets S3.	24 de junho de 2021

Atualizado o cálculo de status de controle agregados e pontuações de segurança padrão	O Security Hub agora calcula o status geral do controle e a pontuação de segurança padrão a cada 24 horas. Para contas de administrador, a pontuação agora indica se cada controle está habilitado ou desabilitado para cada conta.	23 de junho de 2021
Informações atualizadas sobre o tratamento de contas suspensas pelo Security Hub	Foram adicionadas informações sobre como o Security Hub lida com as contas suspensas no AWS.	23 de junho de 2021
Adicionadas guias para exibir os controles habilitados e desabilitados para a conta individual do administrador	Para a conta do administrador, as guias principais na página de detalhes padrão contêm informações agregadas entre as contas. As novas guias Habilitado para esta conta e Desabilitado para esta conta listam as contas que estão habilitadas ou desabilitadas para a conta individual do administrador.	23 de junho de 2021
`java8.al2` adicionado aos parâmetros para `Lambda.2`	No padrão AWS Foundational Security Best Practices, adicionado `java8.al2` aos tempos de execução suportados para o `Lambda.2` controle.	8 de junho de 2021

Novas integrações com o MicroFocus ArcSight NETSCOUT Cyber Investigator	Integrações adicionadas com MicroFocus ArcSight o NETSCOUT Cyber Investigator. MicroFocus ArcSight recebe descobertas do Security Hub. O NETSCOUT Cyber Investigator envia descobertas para o Security Hub.	7 de junho de 2021
Detalhes adicionados para `AWSSecurityHubServiceRolePolicy`	A seção de políticas gerenciadas foi atualizada para adicionar detalhes da política gerenciada existente `AWSSecurityHubServiceRolePolicy` , que é usada pela função vinculada ao serviço do Security Hub.	04 de junho de 2021
Nova integração com o Jira Service Management	O AWS Service Management Connector for Jira envia descobertas para o Jira e as usa para criar problemas no Jira. Quando os problemas do Jira são atualizados, as descobertas correspondentes no Security Hub também são atualizadas.	26 de maio de 2021
A lista de controles compatíveis para a região Ásia-Pacífico (Osaka) foi atualizada	Atualizamos o padrão CIS AWS Foundations e o Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) para indicar os controles que não são suportados na Ásia-Pacífico (Osaka).	21 de maio de 2021

Nova integração com o Sysdig Secure para a nuvem	Adicionada uma integração com o Sysdig Secure para a nuvem. A integração envia as descobertas para o Security Hub.	14 de maio de 2021
Controles adicionados ao padrão AWS Foundational Security Best Practices	Novos controles adicionados para o Amazon API Gateway (ApiGateway.2 e ApiGateway.3), (.4 e CloudTrail .5) CloudTrail, Amazon EC2 (EC2.15 AWS CloudTrail e EC2.16), (.1 e .2), (Lambda.4), Amazon RDS (RDS.12 — RDS.14), Amazon Redshift (AWS Elastic Beanstalk Redshift.7) ElasticBeanstalk, (.7), (.7 AWS Lambda) 3 e .4) e (WAF.1ElasticBeanstalk). AWS Secrets Manager SecretsManager SecretsManager AWS WAF	10 de maio de 2021
Atualizações GuardDuty e controles do Amazon RDS	A gravidade do `GuardDuty.1` e do `PCI.GuardDuty.1` foi alterada de Média para Alta. Um parâmetro `databaseEngines` foi adicionado ao `RDS.8`.	4 de maio de 2021

Adicionados novos detalhes de recursos ao ASFF	Em `Resources.Details` , foram adicionados novos objetos de detalhes de recursos para ACLs de rede do Amazon EC2, sub-redes do Amazon EC2 e ambientes AWS Elastic Beanstalk .	3 de maio de 2021
Campos de console adicionados para fornecer valores de filtro para EventBridge as regras da Amazon	Os novos padrões de filtro predefinidos para EventBridge as regras do Security Hub fornecem campos de console que você pode usar para especificar valores de filtro.	30 de abril de 2021
Adicionou a integração com o AWS Systems Manager Explorer e OpsCenter	O Security Hub agora suporta uma integração com o Systems Manager Explorer OpsCenter e. A integração recebe descobertas do Security Hub e as atualizassas no Security Hub.	26 de abril de 2021
Novo tipo para integrações de produtos	Um novo tipo de integração, `UPDATE_FINDINGS_IN_SECURITY_HUB` , indica que uma integração de produto atualiza as descobertas que recebe do Security Hub.	22 de abril de 2021
A “conta principal” foi alterada para “conta de administrador”	O termo “conta principal” é alterado para “conta de administrador”. O termo também foi alterado no console e na API do Security Hub.	22 de abril de 2021

APIGateway.1 atualizado para substituir HTTP por Websocket	O título, a descrição e a correção do ApiGatewa y.1 foram atualizados. O controle agora verifica o registro de execução da API de WebSocket em vez do log de execução da API HTTP.	9 de abril de 2021
A GuardDuty integração com a Amazon agora é suportada em Pequim e Ningxia	A integração do Security Hub com agora GuardDuty é suportada nas regiões da China (Pequim) e China (Ningxia).	5 de abril de 2021
`nodejs14.x` adicionado aos runtimes compatíveis com o controle Lambda.2	O controle Lambda.2 no Padrão das melhores práticas de segurança básica agora é compatível com o runtime `nodejs14.x` .	30 de março de 2021
Security Hub lançado na Ásia-Pacífico (Osaka)	O Security Hub já está disponível na Região Ásia-Pacífico (Osaka).	29 de março de 2021
Adicionados campos do provedor de descobertas aos detalhes da descoberta	No painel de detalhes da descoberta, a nova seção Campos do provedor de descobertas contém os valores do provedor de descobertas para confiança , criticidade, descobertas relacionadas, gravidade e tipos.	24 de março de 2021

Opção adicionada para receber descobertas confidenciais do Amazon Macie	A integração com o Macie agora pode ser configurada para enviar descobertas confidenciais ao Security Hub.	23 de março de 2021
Fazendo a transição AWS Organizations para gerenciamento de contas	Para clientes que já têm uma conta de administrador com contas de membros, foram adicionadas novas informações sobre como mudar do gerenciamento de contas por convite para o gerenciamento de contas usando Organizations.	22 de março de 2021
Novos objetos no ASFF para obter informações sobre a configuração do Amazon S3 Public Access Block	Em `Resources` , um novo tipo de recurso `AwsS3AccountPublicAccessBlock` e objeto de detalhes fornece informações sobre a configuração do Amazon S3 Public Access Block para as contas. No objeto de detalhes do recurso `AwsS3Bucket` , o objeto `PublicAccessBlockConfiguration` fornece a configuração do Bloco de Acesso Público para o bucket do S3.	18 de março de 2021

Novo objeto no ASFF para permitir a descoberta de provedores para atualizar campos específicos	O novo objeto `FindingProviderFields` no ASFF é usado no `BatchImportFindings` para fornecer valores para `Confidence`, `Criticality`, `RelatedFindings`, `Severity` e `Types`. Os campos originais só devem ser atualizados usando `BatchUpdateFindings`.	18 de março de 2021
Novo objeto `DataClassification` para recursos no ASFF	O novo objeto `Resources.DataClassification` no ASFF é usado para fornecer informações sobre dados confidenciais que foram detectados no recurso.	18 de março de 2021
Valor `CONFIG_RETURNS_NOT_APPLICABLE` adicionado aos códigos de status de conformidade disponíveis	Para o status de conformidade `NOT_AVAILABLE`, o código do motivo `RESOURCE_NO_LONGER_EXISTS` foi removido e o código do motivo `CONFIG_RETURNS_NOT_APPLICABLE` foi adicionado.	16 de março de 2021
Nova política gerenciada para integração com AWS Organizations	Uma nova política gerenciada, `AWSSecurityHubOrganizationsAccess`, fornece às organizações as permissões necessárias para a conta de gestão da organização e para a conta de administrador delegada do Security Hub.	15 de março de 2021

As informações sobre políticas gerenciadas e funções vinculadas a serviços foram movidas para o capítulo Segurança	As informações sobre políticas gerenciadas foram revisadas e expandidas. Tanto as informações da política gerenciada quanto as informações sobre funções vinculadas ao serviço foram transferidas para o capítulo Segurança.	15 de março de 2021
Nova integração com SecureCloud DB	O SecureCloud banco de dados foi adicionado à lista de integrações de terceiros . SecureCloudO DB é uma ferramenta de segurança de banco de dados nativa da nuvem que fornece visibilidade abrangente das posturas e atividades de segurança internas e externas. SecureCloudO banco de dados envia as descobertas para o Security Hub.	4 de março de 2021
Gravidade revisada para os controles CIS 1.1 e CIS 3.1 – CIS 3.14	A gravidade dos controles CIS 1.1 e CIS 3.1 – CIS 3.14 foi alterada para Baixa.	3 de março de 2021
Controle RDS.11 removido	O controle RDS.11 foi removido do Padrão das melhores práticas de segurança básica.	3 de março de 2021
Integração atualizada para o Turbot	A integração do Turbot foi atualizada para enviar e receber descobertas.	26 de fevereiro de 2021

Controles adicionados ao Padrão das melhores práticas de segurança básica	Foram adicionados novos controles para Amazon API Gateway (ApiGatew ay.1), Amazon EC2 (EC2.9 e EC2.10), Amazon Elastic File System (EFS.2), Amazon Service (ES.2 e ES.3), Elastic Load Balancing OpenSearc h (ELB.6) e () (KMS.3). AWS Key Management Service AWS KMS	11 de fevereiro de 2021
Filtro opcional `ProductArn` adicionado à API `DescribeP roducts`	A operação da API `DescribeProducts` agora inclui um parâmetro opcional `ProductArn` . O parâmetro `ProductArn` é usado para identificar a integração de produto específica para a qual retornar detalhes.	3 de fevereiro de 2021
Nova integração com o antivírus para o Amazon S3 da Cloud Storage Security	A integração com o Antivírus para o Amazon S3 envia os resultados da verificação de vírus para o Security Hub como descobertas.	27 de janeiro de 2021
Atualizou o processo de cálculo da pontuação de segurança para contas de administrador	Para uma conta de administr ador, o Security Hub usa um processo separado para calcular a pontuação de segurança. O novo processo garante que a pontuação inclua controles ativados para contas de membros, mas desativados para a conta de administrador.	21 de janeiro de 2021

Novos campos e objetos no ASFF	Adicionado um novo objeto `Action` para monitorar as ações que ocorreram em um recurso. Campos adicionados ao objeto `AwsEc2NetworkInterface` para rastrear nomes DNS e endereços IP. Adicionado um novo objeto `AwsSsmPatchCompliance` aos detalhes do recurso.	21 de janeiro de 2021
Controles adicionados ao Padrão das melhores práticas de segurança básica	Foram adicionados novos controles para Amazon CloudFront (CloudFront.1 a CloudFront .4), Amazon DynamoDB (DynamoDB (DynamoDB.1 a DynamoDB.3), Elastic Load Balancing (ELB.3 a ELB.5), Amazon RDS (RDS.9 a RDS.11), Amazon Redshift (Redshift .1 a Redshift.3 e Redshift.6) e Amazon SHIFT.6) Amazon SNS (SNS.1).	15 de janeiro de 2021

O status do fluxo de trabalho é redefinido com base no estado do registro ou no status de conformidade	O Security Hub redefinirá automaticamente o status do fluxo de trabalho de `NOTIFIED` ou `RESOLVED` para `NEW` se uma descobert a arquivada for ativada ou se o status de conformidade de uma descoberta mudar de `PASSED` para `FAILED`, `WARNING` ou `NOT_AVAIL ABLE` . Essas mudanças indicam que uma investigação adicional é necessária.	7 de janeiro de 2021
Adicionadas informações do `ProductFields` para as descobertas baseadas em controle	Para descobertas geradas a partir de controles, foram adicionadas informaçõ es sobre o conteúdo do objeto `ProductFields` no Formato de descoberta de segurança (ASFF) da AWS .	29 de dezembro de 2020
Atualizações nos insights gerenciados	O título do insight 5 foi alterado. Foi adicionada uma nova percepção, 32, que verifica se há usuários do IAM com atividades suspeitas.	22 de dezembro de 2020
Atualizações nos controles IAM.7 e Lambda.1	No padrão AWS Foundatio nal Security Best Practices , atualizei os parâmetros do IAM.7. O título e a descrição do Lambda.1 foram atualizad os.	22 de dezembro de 2020

Integração expandida com ServiceNow ITSM	A integração do ServiceNow ITSM permite que os usuários criem automaticamente incidentes ou problemas quando uma descoberta do Security Hub é recebida. As atualizações desses incidentes ou problemas resultam em atualizações das descobertas no Security Hub.	11 de dezembro de 2020
Nova integração com o AWS Audit Manager	O Security Hub agora oferece uma integração com o AWS Audit Manager. A integração permite que o Audit Manager receba descobertas baseadas em controle do Security Hub.	8 de dezembro de 2020
Nova integração com o Aqua Security Kube-bench	O Security Hub adicionou uma integração com o Aqua Security Kube-bench. A integração envia as descobertas para o Security Hub.	24 de novembro de 2020
O Cloud Custodian já está disponível nas regiões da China	A integração com o Cloud Custodian já está disponível nas regiões China (Pequim) e China (Ningxia).	24 de novembro de 2020

O `BatchImportFindings` agora pode ser utilizado para atualizar campos adicionais	Anteriormente, não era possível usar o `BatchImportFindings` para atualizar os campos `Confidence`, `Criticality`, `RelatedFindings`, `Severity` e `Types`. Agora, se esses campos não tiverem sido atualizados por `BatchUpdateFindings`, eles poderão ser atualizados por `BatchImportFindings`. Depois de atualizados por `BatchUpdateFindings`, eles não poderão ser atualizados por `BatchImportFindings`.	24 de novembro de 2020
O Security Hub agora está integrado com AWS Organizations	Agora, os clientes podem gerenciar as contas-membro usando a configuração de conta do Organizations. A conta de gestão da organização designa a conta de administrador do Security Hub, que determina quais contas da organização serão habilitadas no Security Hub. O processo de convite manual ainda pode ser utilizado para contas que não fazem parte da organização.	23 de novembro de 2020

Removido o formato de lista de descobertas separada para controles de alto volume	A lista de descobertas de um controle não usa mais o formato da página Descobert as quando há um número muito grande de descobertas.	19 de novembro de 2020
Integrações de terceiros novas e atualizadas	O Security Hub agora oferece suporte a integrações com cloudtamer.io, 3CoreSec, Prowler e Kubernetes Security. StackRox O IBM QRadar não envia mais descobertas. Ele apenas recebe descobertas.	30 de outubro de 2020
Adicionada opção para baixar a lista de descobert as da página de detalhes do controle.	Na página de detalhes do controle, uma nova opção de Download permite baixar a lista de descobertas para um arquivo .csv. A lista baixada respeita todos os filtros que estão na lista. Se você selecionou descobertas específicas, a lista baixada incluirá apenas essas descobertas.	26 de outubro de 2020
Opção adicionada para baixar a lista de controles da página de detalhes padrão.	Na página de detalhes padrão, uma nova opção de Download permite baixar a lista de controle para um arquivo .csv. A lista baixada respeita todos os filtros que estão na lista. Se você selecionou um controle específico, a lista baixada incluirá apenas esse controle.	26 de outubro de 2020

Integrações de parceiros novas e atualizadas	O Security Hub agora está integrado com ThreatModeler o. As seguintes integrações de parceiros foram atualizadas para refletir seus novos nomes de produtos. O Twistlock Enterprise Edition agora é Palo Alto Networks – Prisma Cloud Compute. Também da Palo Alto Networks, o Demisto agora é Cortex XSOAR e o Redlock agora é Prisma Cloud Enterprise.	23 de outubro de 2020
Lançamento do Security Hub na China (Pequim) e na China (Ningxia)	O Security Hub já está disponível nas regiões China (Pequim) e China (Ningxia).	21 de outubro de 2020
Formato revisado para atributos do ASFF e integrações de terceiros	As listas de atributos do ASFF e de integrações de parceiros agora utilizam um formato baseado em lista em vez de tabelas. A sintaxe, os atributos e a taxonomia de tipos do ASFF agora estão em tópicos separados.	15 de outubro de 2020
Página de detalhes padrão redesenhada	A página de detalhes de um padrão habilitado agora exibe uma lista de controles com guias. As guias filtram a lista de controle com base no status do controle.	7 de outubro de 2020
CloudWatch Eventos substituídos por EventBridge	Substituiu as referências à Amazon CloudWatch Events pela Amazon EventBridge.	1º de outubro de 2020

Novas integrações com as séries VM da Blue Hexagon for AWS, Alcide KAudit e Palo Alto Networks.	O Security Hub agora está integrado às séries VM da Blue Hexagon for AWS, Alcide KAudit e Palo Alto Networks. O Blue Hexagon for AWS e o KAudit enviam descobert as para o Security Hub. O VM-Series recebe todas as descobertas do Security Hub.	30 de setembro de 2020
Objetos de detalhes de recursos novos e atualizados no ASFF	Foram adicionados novos objetos `Resources .Details` para `AwsApiGat ewayRestApi`, `AwsApiGatewayStage`, `AwsApiGatewayV2Api`, `AwsApiGatewayV2Stage`, `AwsCertificateMana gerCertificate`, `AwsElbLoadBalancer`, `AwsIamGroup` e `AwsRedshi ftCluster`. Detalhes adicionados aos objetos `AwsCloudFrontDistr ibution`, `AwsIamRole` e `AwsIamAccessKey`.	30 de setembro de 2020
Novo atributo `ResourceR ole` para recursos no ASFF para rastrear se um recurso é um ator ou um alvo.	O atributo `ResourceRole` para recursos indica se o recurso é o alvo da atividade de descoberta ou o autor da atividade de descoberta. Os valores válidos são `ACTOR` e `TARGET`.	30 de setembro de 2020

Adicionou o AWS Systems Manager Patch Manager às integrações AWS de serviços disponíveis	AWS Systems Manager O Patch Manager agora está integrado ao Security Hub. O Patch Manager envia as descobertas ao Security Hub quando as instâncias da frota de um cliente não estão em conformidade com seu padrão de conformidade de patches.	22 de setembro de 2020
Foram adicionados novos controles ao padrão AWS Boundational Security Best Practices	Foram adicionados novos controles para os seguintes serviços: Amazon EC2 (EC2.7 e EC2.8), Amazon EMR (EMR.1), IAM (IAM.8), Amazon RDS (RDS.4 a RDS.8), Amazon S3 (S3.6) e (.1 e .2). AWS Secrets Manager SecretsManager SecretsManager	15 de setembro de 2020
Novas chaves de contexto para a política do IAM para controlar o acesso aos campos `BatchUpdateFindings`	As políticas do IAM agora podem ser configuradas para restringir o acesso a campos e valores de campo ao usar `BatchUpdateFindings` .	10 de setembro de 2020
Acesso expandido ao `BatchUpdateFindings` para contas-membro	Por padrão, as contas de membros agora têm o mesmo acesso que `BatchUpdateFindings` as contas de administrador.	10 de setembro de 2020

Novos controles para AWS KMS o Padrão Fundamental de Melhores Práticas de Segurança	Foram adicionados dois novos controles (KMS.1 e KMS.2) ao Padrão de melhores práticas de segurança básica. Os novos controles verificam se as políticas do IAM restringem o acesso às ações de AWS KMS descriptografia.	9 de setembro de 2020
Foram removidas as descobertas em nível de conta para controles	O Security Hub não gera mais descobertas em nível de conta para um controle. Somente descobertas em nível de recurso são geradas.	1.º de setembro de 2020
Novo objeto PatchSummary no ASFF	O objeto `PatchSummary` foi adicionado ao ASFF. O objeto `PatchSummary` fornece informações sobre a conformidade do patch de um recurso em relação a um padrão de conformidade selecionado.	1.º de setembro de 2020
Página de detalhes do controle redesenhada	A página de detalhes dos controles foi redesenhada. A lista de descoberta de controles fornece guias para permitir que você filtre rapidamente a lista com base no status de conformidade. Você também pode ver rapidamente as descobertas suprimidas. Cada entrada fornece acesso a detalhes adicionais sobre o recurso de busca, a AWS Config regra e as notas da descoberta.	28 de agosto de 2020

Novas opções de filtro para descobertas	No filtro de descobertas, é possível filtrar utilizando a opção não é para localizar as descobertas para as quais o valor do campo não é igual ao valor do filtro. É possível usar a opção não começa com para localizar descobertas para as quais um valor de campo não começa com o valor de filtro especificado.	28 de agosto de 2020
Novos objetos de detalhes de recursos no ASFF	Foram adicionados novos objetos `Resources.Details` para os seguintes tipos de recursos: `AwsDynamoDbTable`, `AwsEc2Eip`, `AwsIamPolicy`, `AwsIamUser`, `AwsRdsDbCluster`, `AwsRdsDbClusterSnapshot`, `AwsRdsDbSnapshot` e `AwsSecretsManagerSecret`	18 de agosto de 2020
Nova integração com o RSA Archer	O Security Hub agora está integrado ao RSA Archer. O RSA Archer recebe todas as descobertas do Security Hub.	18 de agosto de 2020
Novo campo de descrição para AwsKmsKey	Um campo `Description` foi adicionado ao objeto `AwsKmsKey` em `Resources.Details`.	18 de agosto de 2020

Campos adicionados ao AwsRdsDbInstance	Foram adicionados vários atributos ao objeto `AwsRdsDbInstance` em `Resources.Details` .	18 de agosto de 2020
Atualização da forma como o Security Hub determina o status geral de um controle	Para controles que não têm descobertas, o status é Sem dados em vez de Desconhecido. O status do controle inclui descobertas em nível de conta e em nível de recurso. O status de controle não usa o status do fluxo de trabalho das descobertas, exceto para ignorar as descobertas suprimidas.	13 de agosto de 2020
Atualização da forma como o Security Hub calcula a pontuação de segurança de um padrão	Ao calcular a pontuação de segurança de um padrão, o Security Hub agora ignora os controles com o status Sem dados. A pontuação de segurança é a proporção dos controles aprovados em relação aos controles habilitados, excluindo os controles sem dados.	13 de agosto de 2020
Nova opção para habilitar automaticamente novos controles em padrões habilitados	Adicionada uma opção de Configurações para habilitar automaticamente novos controles nos padrões que estão habilitados. Também é possível usar a operação `UpdateSecurityHubConfiguration` da API para configurar essa opção.	31 de julho de 2020

Novos controles para o padrão PCI DSS (Payment Card Industry Data Security Standard)	Foram adicionados novos controles ao Padrão PCI DSS. Os identificadores dos novos controles são PCI.DMS.1 , PCI.EC2.5, PCI.EC2.6, PCI.ELBV2.1, PCI. GuardDuty 1., PCI.IAM.7, PCI.IAM.8 , PCI.S3.5, PCI.S3.6, PCI. SageMaker.1, PCI.SSM.2 e PCI.SSM.3.	29 de julho de 2020
Controles novos e atualizados para o Padrão das melhores práticas de segurança básica	Foram adicionados novos controles ao Padrão das melhores práticas de segurança básica. Os identific adores dos novos controles são AutoScaling .1, DMS.1, EC2.4, EC2.6, S3.5 e SSM.3. O título do ACM.1 foi atualizad o e o valor do parâmetro `daysToExpiration` foi alterado para 30.	29 de julho de 2020
Novo objeto `Vulnerabi lities` no ASFF	Foi adicionado o objeto `Vulnerabilities` , que fornece informações sobre as vulnerabilidades associadas à descoberta.	1º de julho de 2020
Novos objetos `Resource. Details` no ASFF para grupos do Auto Scaling, volumes do EC2 e VPCs do EC2	Os objetos `AwsAutoSc alingAutoScalingGr oup` , `AWSEc2Volume` e `AwsEc2Vpc` foram adicionad os a `Resource.Details` .	1º de julho de 2020

Novo objeto `NetworkPath` no ASFF	Foi adicionado o objeto `NetworkPath`, que fornece informações sobre um caminho de rede relacionado à descoberta.	1º de julho de 2020
Solucionar as descobertas automaticamente quando `Compliance.Status` for `PASSED`	Para as descobertas de controles, se `Compliance.Status` for `PASSED`, o Security Hub definirá `Workflow.Status` automaticamente como `RESOLVED`.	24 de junho de 2020
AWS Command Line Interface exemplos	AWS CLI Sintaxe e exemplos adicionados para várias tarefas do Security Hub. Inclui a habilitação do Security Hub, a gestão de insights, de padrões e controles, de integrações de produtos e desabilitação do Security Hub.	24 de junho de 2020
Novo atributo `Severity.Original` no ASFF	Adição do atributo `Severity.Original`, que é a gravidade original do provedor de descoberta. Isso substitui o atributo defasado `Severity.Product`.	20 de maio de 2020
Novo objeto `Compliance.StatusReasons` no ASFF para obter detalhes sobre o status de um controle	Adição do objeto `Compliance.StatusReasons`, que fornece contexto adicional para o status atual de um controle.	20 de maio de 2020

Novo AWS padrão básico de melhores práticas de segurança	Foi adicionado o novo padrão AWS Foundational Security Best Practices, que é um conjunto de controles que detectam quando suas contas e recursos implantados se desviam das melhores práticas de segurança.	22 de abril de 2020
Nova opção de console para atualizar o status do fluxo de trabalho de uma descoberta	Adicionadas informações sobre como usar o console ou a API do Security Hub para definir o status do fluxo de trabalho para descobertas.	16 de abril de 2020
Nova API `BatchUpdateFindings` para atualizações de clientes para descobertas	Adicionadas informações sobre como usar `BatchUpdateFindings` para atualizar informações relacionadas ao processo de investigação de uma descoberta. `BatchUpdateFindings` substitui `UpdateFindings`, que está defasado.	16 de abril de 2020

Atualizações no AWS Security Finding Format (ASFF)	Adição de vários novos tipos de recurso. Adição de um novo atributo `Label` ao objeto `Severity`. `Label` destina-se a substituir o campo `Normalized` . Adição de um novo objeto `Workflow` para rastrear o processo de uma investigação em uma descoberta. `Workflow` contém um atributo `Status`, que substitui o atributo `Workflowstate` existente.	12 de março de 2020
Atualizações na página Integrações	Atualizado para refletir as alterações na página Integrations (Integrações). Para cada integração, a página agora mostra a categoria de integração e se cada integração envia ou recebe descobertas do Security Hub. Ela também fornece as etapas específicas necessárias para permitir cada integração.	26 de fevereiro de 2020
Novas integrações de produtos de terceiros	Foram adicionadas as seguintes novas integrações de produtos: Cloud Custodian, FireEye Helix, Forcepoint CASB, Forcepoint DLP, Forcepoint NGFW, Rackspace Cloud Native Security e Vectra.ai Cognito Detect.	21 de fevereiro de 2020

Novo padrão de segurança para o PCI DSS (Payment Card Industry Data Security Standard)	Adicionado o padrão de segurança do Security Hub para o PCI DSS (Payment Card Industry Data Security Standard). Quando esse padrão está habilitado, o Security Hub realiza verificaç ões automatizadas dos controles relacionados aos requisitos do PCI DSS.	13 de fevereiro de 2020
Atualizações no AWS Security Finding Format (ASFF)	Adição de um campo de requisitos relacionados para controles de padrões. Adição de novos tipos de recursos e novos detalhes de recursos. Agora o ASFF também permite que você forneça até 32 recursos.	5 de fevereiro de 2020
Nova opção para desabilit ar controles de padrão de segurança individuais	Adição de informações sobre como controlar se cada controle de padrão de segurança individual está habilitado.	15 de janeiro de 2020
Atualizações de terminologia e conceitos	Atualização de algumas descrições e adição de novos termos a Terminologia e conceitos.	21 de setembro de 2019
AWS Versão de disponibi lidade geral do Security Hub	Atualizações de conteúdo para refletir as melhorias feitas no Security Hub durante o período de visualização.	25 de junho de 2019

Etapas de remediação adicionadas para verificações do CIS Foundations AWS	Foram adicionadas etapas de remediação aos padrões de segurança suportados no AWS Security Hub.	15 de abril de 2019
Versão prévia do AWS Security Hub	Publicada a versão de visualização do Guia do usuário do AWS Security Hub.	18 de novembro de 2018

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.